S. HRG. 107–852

PRIVACY, IDENTITY THEFT, AND THE PROTECTION OF YOUR PERSONAL INFORMATION IN THE 21ST CENTURY

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

FEBRUARY 14, 2002

Serial No. J–107–60

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
85–061 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts	ORRIN G. HATCH, Utah
JOSEPH R. BIDEN, JR., Delaware	STROM THURMOND, South Carolina
HERBERT KOHL, Wisconsin	CHARLES E. GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ARLEN SPECTER, Pennsylvania
RUSSELL D. FEINGOLD, Wisconsin	JON KYL, Arizona
CHARLES E. SCHUMER, New York	MIKE DEWINE, Ohio
RICHARD J. DURBIN, Illinois	JEFF SESSIONS, Alabama
MARIA CANTWELL, Washington	SAM BROWNBACK, Kansas
JOHN EDWARDS, North Carolina	MITCH MCCONNELL, Kentucky

BRUCE A. COHEN, *Majority Chief Counsel and Staff Director*
SHARON PROST, *Minority Chief Counsel*
MAKAN DELRAHIM, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

DIANNE FEINSTEIN, California, *Chairperson*

JOSEPH R. BIDEN, JR., Delaware	JON KYL, Arizona
HERBERT KOHL, Wisconsin	MIKE DEWINE, Ohio
MARIA CANTWELL, Washington	JEFF SESSIONS, Alabama
JOHN EDWARDS, North Carolina	MITCH MCCONNELL, Kentucky

DAVID HANTMAN, *Majority Chief Counsel*
STEPHEN HIGGINS, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

SUBMISSIONS FOR THE RECORD

PRIVACY, IDENTITY THEFT, AND THE PROTECTION OF YOUR PERSONAL INFORMATION IN THE 21ST CENTURY

THURSDAY, FEBRUARY 14, 2002

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:37 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Dianne Feinstein, presiding.

Present: Senators Feinstein, Cantwell, and Kyl.

Chairperson FEINSTEIN. In the interest of time, I think we will probably start. The Ranking Member has been delayed. He will be along very shortly, but Senator Gregg, we are delighted to have you here. I know Senator Kyl would like also to hear your remarks, probably more than my remarks, so why do I not go ahead and quickly make my remarks, and then in the meantime, he should be here to hear yours, if that is agreeable with you.

Senator KYL. I appreciate it. Whatever the Chairman wishes to do is fine with me.

OPENING STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Chairperson FEINSTEIN. All right. Let me just begin then by thanking you for your work on the Social Security numbers. I know you are going to speak about that and I will let you do it, but it has been a great pleasure for us to be able to work with you and I want you to know that.

In 1928, Supreme Court Justice Louis Brandeis described privacy, and I quote, as the "right most valued by civilized people," and he defined it simply as the right to be left alone. With the advent of instant communication, the preservation of this right, I very deeply believe, is at risk. There are ominous signs that we are losing control over our personal information. Here are just a few examples.

Some websites store and sell data on the most intimate aspects of our personal lives—where we live, the value of our homes, the mortgages that we have, our financial histories, and even our medical conditions. Your Social Security number today can be purchased for as little as $25 on the Internet. One medical information service has, and can distribute at will, data bases containing the

phone number, the gender, and the address of 368,000 people with clinical depression or 3.3 million people with allergies. And according to one privacy advocate, a typical person's name and address are known to 500 companies or more. So without a doubt, the threat posed by the misuse of personal information is there and needs to be addressed.

First, as the General Accounting Office will report today, identity theft crimes continue to surge. Identity theft occurs when another person literally steals your identity for profit or other illicit motive. Recently, the Federal Trade Commission reported that identity theft was the largest complaint on the Commission's consumer complaint list last year, representing 42 percent of its 204,000 complaints. Some privacy groups estimate that as many as 750,000 people a year are victims of this crime.

Second, stalkers and others with criminal intent can increase their ability to harm their victims by gaining access to their personal information. We will hear today from Susan Fisher, whose brother was killed by an ex-girlfriend who stalked him by gaining access to his personal records.

Third, many people simply do not want their personal information, such as the amount of their bank account, the type of medications they take, or their home address, widely shared with other people, and I deeply believe that they have that right to privacy.

Some have suggested that in light of the ongoing war on terror, privacy needs to take a backseat to issues of safety and security. I strongly challenge this view. Protecting basic consumer privacy is compatible with enhanced security. In fact, the goals of privacy and security are often complementary.

The recent acts of terror show how personal information can be misused to advance terrorist or other criminal activities. According to the Social Security Administration, six of the 19 hijackers in the September 11 attack were using Social Security numbers illegally. Moreover, an al Qaeda associate recently testified that the organization trained its operatives how to obtain stolen licenses, credit cards, and Social Security numbers.

It also must be acknowledged that efforts to protect privacy must be balanced with the benefits so many Americans enjoy because of the widespread use of personal information. Many of us appreciate the ability to get instant credit, locate long-lost college friends, purchase items swiftly on the Internet, or be notified of products that might interest us. Therefore, I believe it is critical that any initiative on privacy strike a proper balance, and I think we have crafted legislation to do just that.

Today's hearing will discuss the need for comprehensive legislation to deter identity theft and protect personal privacy. It will specifically address S. 1055, the Privacy Act of 2001. I want to take just a brief moment to describe the bill because it sets out where I stand on privacy.

The Privacy Act of 2001 creates a two-tiered system of privacy protection that recognizes that not all information is equally sensitive. For your most sensitive information, the bill requires that companies get your consent before they sell the data. It is called opt-in. For example, under the Privacy Act, you must give your consent before a bank can sell information about your account bal-

ance, the stocks you own, your spending habits, or other personal financial data. That is opt-in.

You must give your consent before a school, university, life insurer, or any other entity sells or markets your sensitive health data, such as your mental state, your disease status, or the prescriptions that you buy. That is opt-in.

You must give your consent before the sensitive information on your driver's license, such as your driver's license number, your height, your weight, your sex or birthdate, can be sold. That is opt-in.

The Privacy Act will also stop the practice of companies selling Social Security numbers to any member of the public who wants your number.

However, to reflect the legitimate needs of business, the Privacy Act proposes a lower threshold for the sale of less-sensitive information, such as a person's name and address. Under this lower threshold, businesses must give notice of their intent. They must give notice of their intent to use this information. After giving notice, the business can sell this less-sensitive data unless the individual tells them not to. That is opt-out.

We have an impressive roster of witnesses at today's hearing. As I mentioned, Senator Judd Gregg, who has shown a lot of leadership on this subject, will testify as a first panel on the privacy of Social Security numbers.

In the second panel, the GAO will give preliminary results of its year-long study of identity theft.

In the third panel, we will hear testimony on this bill from Susan Fisher of the Doris Tate Crime Victims Bureau, Frank Torres of the Consumers Union, Doug Comer of Intel, and John Avila of the Disney Corporation.

Senator Kyl should be along momentarily, but in the interim, Senator Gregg, I will turn to you now.

Senator GREGG. Thank you, Senator.

Chairperson FEINSTEIN. Before you do, Senator, if I might just put in the record the statement of Laura Nyquist, the Chief Privacy Officer of NCR Corporation.

I would also like to include a statement from the American Medical Association.

Finally, I will include a statement by the Privacy Times, the testimony of Evan Hendricks. I would like to add these to the record.

Please go ahead, Senator.

STATEMENT OF HON. JUDD GREGG, A U.S. SENATOR FROM THE STATE OF NEW HAMPSHIRE

Senator GREGG. Thank you, Senator. I appreciate the courtesy of your inviting me to testify at this hearing, which is an extremely important hearing on a very topical subject, and I congratulate you for all the work you have put into this issue as certainly one of the leaders in the Congress and the country on the issue of how to protect people's privacy. I have enjoyed very much having a chance to work with you on this issue.

Chairperson FEINSTEIN. Thank you.

Senator GREGG. I might just start by explaining how I became involved in this issue. On October 15, 1999, a constituent of mine,

Amy Boyer, who was a young woman who came from my hometown of Nashua, New Hampshire, was killed by a man who had gone on the Internet and taken possession of her Social Security number and other personal information by using access which he had obtained through the Internet.

Until recently, we had thought that he had only obtained the Social Security number in order to stalk Amy, but unfortunately, it now turns out from court documents that he had paid a $75 fee to a company and that company had then used what they called a pretexter, who had posed as an insurance official and had called her and obtained personal information from her on the pretext that he was going to give her an insurance award, I guess. As a result of collecting that information, they then disseminated it to this individual over the Internet. The whole transaction, it appears, occurred via the Internet.

Unfortunately, the pretexter's approach worked. Amy Boyer was stalked and she was killed by this individual.

As a result of this extraordinarily tragic event and countless others which have come to my attention and which Senator Feinstein has mentioned have come to her attention, I believe that we should make some changes in how information, personal information, is conveyed and used in the marketplace and specifically relative to Social Security numbers. Senator Feinstein and I have worked very closely on this issue.

We have developed language, which is S. 848, the Social Security Number Misuse Prevention Act. This Act is part of the bill which you are discussing here today, S. 1055, as I understand, I believe the second title of that Act. Although I am very interested in the other issues which are raised by your bill, I want to confine myself to the Social Security issue, because this is where I have concentrated most of my time, and I feel a deep personal responsibility as the representative of the family of Amy Boyer to do something in this area, so I have committed a considerable amount of time trying to reach legislation which will accomplish this.

In drafting S. 848, there really is only one primary goal and that is to ensure that people would not be able to purchase Social Security numbers and that companies would not be able to sell Social Security numbers without an individual giving their consent. In introducing this legislation, Senator Feinstein and I have worked hard to strike a delicate balance between legitimate business and other lawful uses of Social Security numbers, of which there are many, and our shared desire to limit general public access to Social Security numbers because of the significant risk of invasion of privacy that comes from people being able to obtain your Social Security number.

We have to understand that, like it or not, the Social Security number has become a national identifier, and in many instances, it is the only way to ensure accurate identification of people. Health care providers use Social Security numbers to maintain our health records to ensure we are receiving the services we need and we have a right to. Banks and financial institutions use them to prevent fraud against individuals. Social Security numbers tell them that a loan applicant is exactly who he or she says she is.

The National Center for Missing and Exploited Children and the Association for Children, the enforcement of support, use Social Security numbers to track down kidnappers and deadbeat dads. Big Brothers/Big Sisters of America uses Social Security numbers to do background checks on volunteers to make sure they are not people who might harm the children who they are working with.

A truly blanket prohibition, therefore, on Social Security numbers would probably undermine a great deal of legitimate uses. In reality, nobody wants to do this, so we worked on striking a balance, myself and Senator Feinstein. I believe that we have maybe not a perfect product, but we have succeeded in identifying and responding to the key issues in a thoughtful and, I believe, constructive way on this matter.

Under the legislation, obtaining a Social Security number with wrongful intent is illegal. Under the legislation, no Social Security number may be displayed, sold, purchased without the individual's consent, except in the cases involving public health, national security, law enforcement, and certain limited business-to-business transactions. No individual may be required to provide a Social Security number when purchasing a commercial good or services unless the Social Security number is absolutely necessary as defined by the Act, and the definition is limited.

Under the legislation, within 1 year, Social Security numbers may not appear on any driver's license, motor vehicle registration, or any other document issued to an individual for the purposes of identification of that individual. The obvious reason for that is that as you are going through an airport or something and you have to show your driver's license, you should not have to disclose your Social Security number.

Under the bill, within 3 years, Social Security numbers may not appear on checks issued for payment by Federal, State, or local agencies, Federal Government agencies.

Finally, on the issuance of public records, which was and remains a very difficult issue, we worked to strike a balance between maintaining public access and limiting the potential for harm that comes with that access. To that end, we considered the impact of possibly having to redact Social Security numbers from thousands, if not millions, of public documents. This would be a hugely expensive and labor intensive task and it is unclear whether we would in any significant way further reduce the illegal activity we are trying to prevent. In other words, it is unclear whether the administrative burden and the cost would outweigh the potential benefit, and this is a very real concern.

Under our compromise proposal, there is no requirement for redaction of Social Security numbers until that document is sold or displayed to the public, and then only where the number appears on the face of the document or in a highly consistent and predictable place inside the document.

For example, records which are known to always contain a Social Security number on a particular page, and in that case, the number would need to be redacted before that document could be sold to the public. There is no requirement that the Records Office would have to screen through documents that might incidentally contain a Social Security number.

Madam Chairman, every year, as many as 700,000 instances of identity theft are reported. Limiting availability of Social Security numbers is one important way we can address this issue. S. 848 as it is incorporated into your bill is a well thought out, tightly woven piece of legislation that effectively recognizes and balances the many concerns surrounding the issue of Social Security numbers and their theft and misuse. Passing this legislation is one of the most important things that the Congress can do this year to reduce identity theft and protect individual privacy while permitting the continued legitimate and limited use of Social Security numbers.

Madam Chairman, I thank you for the chance to testify today.

Chairperson FEINSTEIN. Thanks very much, Senator Gregg. I very much appreciate your comments. I think we have got a very secure and good part of this bill, and perhaps you and I—I know Senator Kyl was unavoidably detained. He is always here faithfully on the dot. So perhaps you and I can talk with him a little bit about it—

Senator GREGG. We will capture him somewhere.

Chairperson FEINSTEIN [continuing]. Because I hope to move this thing along. But thank you very much for your leadership and for being here today.

Senator GREGG. I appreciate your courtesy.

Chairperson FEINSTEIN. I very much appreciate it.

As you can probably tell from the buzzer and the beeper, there is a vote going on, but what I would like to do is begin the testimony and then perhaps 10 minutes into it, if Senator Kyl is not able to be here, we will just take a brief break and I can run down and vote and come back.

Let me begin with panel two and ask Mr. Richard Stana please to come and have a seat. Mr. Stana is the Director for Justice Issues at the GAO. During his 25-year career with GAO, he has directed reviews on a wide variety of complex military and domestic issues in headquarters, the field, and overseas offices. Most recently, he has directed the GAO's work relating to law enforcement, drug control, immigration, corrections, court administration, and election systems. He has received numerous awards throughout his career and he has been active in many civic and community organizations, as well as his work with the Federal Government.

Mr. Stana, we are delighted to have you here and we welcome your testimony.

STATEMENT OF RICHARD M. STANA, DIRECTOR, JUSTICE ISSUES, GENERAL ACCOUNTING OFFICE; ACCOMPANIED BY DANNY R. BURTON, ASSISTANT DIRECTOR, DALLAS FIELD OFFICE, GENERAL ACCOUNTING OFFICE; AND RONALD J. SALO, SENIOR ANALYST, DALLAS FIELD OFFICE, GENERAL ACCOUNTING OFFICE

Mr. STANA. Thank you very much, Madam Chairman. I am pleased to be here today to discuss the preliminary results of our study on the extent or prevalence of identity theft and its cost to the financial services industry, to victims, and to the Federal justice system.

With me at the table are Dan Burton, Assistant Director on this assignment, and Ron Salo, the lead analyst. Behind us is Robert Rivas, who contributed substantially to this product.

As a matter of definition, identity theft involves stealing another person's personal identifying information, such as their Social Security number, date of birth, or mother's maiden name, and then using the information to create a false identity document to fraudulently establish credit and run up debt or to take control of existing financial accounts in order to make unauthorized purchases.

My prepared statement discusses in detail our preliminary results. I would like to take this opportunity to briefly summarize a few important points and comment on several facets of identity theft that are addressed in S. 1055, the Privacy Act of 2001.

The first point is that although identity theft numbers are not easily captured and sometimes reflect different viewpoints, the statistics we compiled indicate that identity theft continues to rise. Data from national credit bureaus show that the number of fraud alerts placed on consumer accounts is increasing. The data ranges from an estimated low of about 30,000 victims annually to an estimated high of about 178,000 victims annually. Although these statistics are significant, the lower-end figure understates the magnitude of the problem because it does not take into account both account takeover victims and identity theft victims. Neither estimate includes victims whose wallets or purses were stolen but who did not call the credit bureau.

The most current statistics compiled by the FTC's Identity Theft Data Clearinghouse show that about 3,000 identity theft victims call each week. Additionally, the Social Security Administration's IG Fraud Hotline received over 65,000 allegations of Social Security number misuse in fiscal year 2001. About four of five SSN misuse allegations relate directly to identity theft.

Statistics on arrests, investigations, and dollar losses compiled by leading Federal law enforcement agencies, that is, the Secret Services, the SSA IG, the IRS, the FBI, and the Postal Inspection Service, all show an increasing trend in criminal activity, as well as increasing law enforcement and prosecutorial activity. But these statistics do not indicate the full magnitude of victimization because not all incidents of identity theft are reported and investigated, nor do these statistics reflect activity at the State and local levels, where most identity theft allegations are reported.

My second point is that the costs of identity theft to the financial services industry, to victims, and to law enforcement are substantial. The cost to the financial services industry in terms of documented bank check fraud and Visa and MasterCard total payment card fraud is about $1.8 billion from domestic operations alone. Check fraud losses by banks for individual accounts, considering both actual losses and loss avoidance, reached an estimated $2.2 billion in 1999, which was twice the amount of losses in 1997, according to the ABA. On average, about $1 in $3 of check fraud losses are identity theft related.

Visa and MasterCard reported two categories of payment card fraud, account takeovers and fraudulent applications, which they associate closely with identity theft. These rose 43 percent, from about $80 million in 1996 to about $114 million in 2000. In the

view of law enforcement, however, virtually all categories of payment card fraud encompass identity theft. Under their broader definition, the two associations' combined total fraud losses from domestic operations alone rose 45 percent from 1996 to 2000. These statistics do not include data from other firms, such as American Express, Diners Club, and Discover, that comprise about 25 percent of general purpose card markets.

It should be noted also that we found no comprehensive data on direct fraud losses to the retail, insurance, or other industries.

The cost of identity theft to individual victims can cause potential severe emotional distress as well as economic harm. Victims often feel personally violated and report significant amounts of time trying to resolve the problems caused by identity theft, problems such as bounced checks, loan denials, credit card application rejections, and debt collection harassment.

The most common harm reported to the FTC was denied credit or other financial services. On the extreme end, victims had been subjected to criminal investigations, arrest, or even conviction. In terms of monetary harm, the FTC reported that about 15 percent of the victims reporting a loss alleged losing more than $5,000.

The cost to the Federal criminal justice system to investigate, prosecute, incarcerate, and supervise offenders is difficult to capture because information systems do not separately track such costs. Nevertheless, in response to our request, the FBI and Secret Service indicated the average cost of an investigative matter was between $15,000 and $20,000. The average white collar prosecution costs about $11,000. And the average incarceration costs, about $17,000 per inmate, and annual supervision, about $3,000 per offender.

Let me turn now—I am sorry?

Chairperson FEINSTEIN. I am going to try to wait, ask them to keep the vote open. You continue, and then we will recess when you are finished.

Mr. STANA. Turning now to other aspects of identity theft, although the scope of our work for the subcommittee did not include an evaluation of various legislative proposals, we did compile information that offers perspectives on various provisions in S. 1055 that are designed to address some aspects of identity theft.

For example, a major component of identity theft is acquiring personal identifiers, such as SSNs or drivers' licenses, to build false identities. According to a 1999 study by the Sentencing Commission, drivers' licenses and SSNs are the identification means most frequently used to generate or breed other fraudulent identifiers. As you know, S. 1055 would prohibit the use of SSNs and drivers' licenses for motor vehicle registration documents.

Another potential source of personal identifiers for identity thieves is the personal financial information sold by financial institutions to non-affiliated third parties. Gramm-Leach-Bliley established the opt-out standard which you discussed before. S. 1055 would amend Gramm-Leach-Bliley to provide consumers an opt-in standard, whereby a bank would need prior consent of the consumers before selling personal financial information to non-affiliated parties.

Resource levels and competing priorities can limit any one level of government's capacity, including the Federal Government's capacity, to address identity theft crimes. S. 1055 would empower State attorneys general to enforce the Privacy Act. Although Gramm-Leach-Bliley does not have a similar provision, the Act's legislative history indicates that earlier versions of the House and Senate bills included a similar State enforcement authority, which was dropped in conference.

And finally, in a similar vein, resource constraints and dollar threshold levels have limited the numbers and types of cases that Federal law enforcement agencies have investigated. One type of case that has not often been investigated involves SSN misuse. Currently, the SSA IG devotes the vast majority of its investigative resources to program integrity priority areas rather than SSN misuse cases. SSN misuse allegations increased more than five-fold, to about 65,000, in 2001. S. 1055 would give SSA the authority to impose civil monetary penalties for SSN misuse. Now, it is not clear how the SSA IG would carry out this new authority or how many additional resources it would require and at what cost.

Madam Chairman, this concludes my oral statement. We would be pleased to address any questions you or other members of the subcommittee may have.

[The prepared statement of Mr. Stana follows:]

STATEMENT OF RICHARD M. STANA, DIRECTOR, JUSTICE ISSUES, U.S. GENERAL ACCOUNTING OFFICE, WASHINGTON, D.C.

Madam Chairwoman and Members of the Subcommittee:

I am pleased to be here today to discuss the preliminary results of our ongoing study requested by the Subcommittee and Senator Charles Grassley to develop information on the extent or prevalence of identity theft and its cost to the financial services industry, victims, and the federal criminal justice system. Generally, identity theft involves "stealing" another person's personal identifying information such as Social Security number (SSN), date of birth, and mother's maiden name and then using the information to fraudulently establish credit, run up debt, or to take over existing financial accounts. Although not specifically or comprehensively quantifiable, the prevalence and cost of identity theft seem to be increasing, according to the available data we reviewed and many officials of the public and private sector entities we contacted. Given such indications, most observers agree that identity theft certainly warrants continued attention, encompassing law enforcement as well as prevention efforts. Various recently introduced bills, including S. 1055 (Privacy Act of 2001), have provisions designed to enhance such efforts. While the scope of our work did not include an evaluation of S. 1055, we did compile information that could be useful in discussing related issues, and my testimony today will offer perspectives on several identity theft-related provisions of the bill.

To obtain the most recent statistics on the incidence and societal cost of identity theft, we interviewed responsible officials and reviewed documentation obtained from the Department of Justice and its components, including the Executive Office for U.S. Attorneys (EOUSA) and the Federal Bureau of Investigation (FBI); the Department of the Treasury and its components, including the Secret Service and the Internal Revenue Service (IRS); the Social Security Administration's (SSA) Office of the Inspector General (OIG); the Postal Inspection Service; and the Federal Trade Commission (FTC). Also, we contacted representatives of the three national consumer reporting agencies (commonly referred to as "credit bureaus") and two payment card associations (MasterCard and Visa). Further, at our request and with the consent of the victims, FTC provided us with the names and telephone numbers of 10 victims to interview. According to FTC staff, the sample of 10 victims was selected to illustrate a range in the extent and variety of the identity theft activities reported by victims. The experiences of these 10 victims are not statistically representative of all victims.

BACKGROUND

Since our earlier report in May 1998,[1] various actions particularly passage of federal and state statutes have been taken to address identify theft. Later that year, Congress passed the Identity Theft and Assumption Deterrence Act of 19098 (the "Identity Theft Act").[2] Enacted in October 1998, the federal statute made identify theft a separate crime against the person whose identity was stolen, broadened the scope of the offense to include the misuse of information as well as documents, and provided punishment generally, a fine or imprisonment for up to 15 years or both. Under U.S. Sentencing Commission guidelines even if (1) there is no monetary loss and (2) the perpetrator has no prior criminal convictions a sentence of from 10 to 16 months incarceration can be imposed. Regarding state statutes, at the time of our 1998 report, very few states had specific laws to address identity theft. Now, less than 4 years later, a large majority of states have enacted identify theft statues.

PREVALENCE OF IDENTITY THEFT

As we reported in 1998, there are no comprehensive statistics on the prevalence of identity theft or identity fraud. Similarly, during our current review, various officials noted that precise, statistical measurement of identity theft trends is difficult for number of reasons. Generally, federal law enforcement agencies do not have information systems that specifically track identity theft cases. For example, while the amendments of the Identity Theft Act are included as subsection (a)(7) of section 1028, Title 18 of the U.S. Code, EOUSA does not have comprehensive statistics on offenses charged specifically under that subsection because docketing staff are asked to record cases under only the U.S. Code section, not the subsection or the sub-subsection. Also, the FBI and the Secret Service said that identity theft is not typically a stand-alone crime; rather, it is almost always a component of one or more white-collar or financial crimes, such as bank fraud, credit card or access device fraud, or the use of counterfeit financial instruments.

Nonetheless, a number of data sources can be used as proxies for gauging the prevalence of identity theft. These sources can include consumer complaints and hotline allegations, as well as law enforcement investigations and prosecutions of identity theft-related crimes such as bank fraud and credit card fraud. Each of these various sources or measures seems to indicate that the prevalence of identity theft is growing.

CONSUMER REPORTING AGENCIES: AN INCREASING NUMBER OF FRAUD ALERTS ON CONSUMER FILES

According to the consumer reporting agency officials that we talked with, the most reliable indicator of the incidence of identity theft is the number of 7-year fraud alerts placed on consumer credit files. Generally, fraud alerts constitute a warning that someone may be using the consumer's personal information to fraudulently obtain credit. Thus, a purpose of the alert is to advise credit grantors to conduct additional identity verification or contact the consumer directly before granting credit. One of the three consumer reporting agencies that we contacted estimated that its 7-year fraud alerts involving identity theft increased 36 percent over 2 recent years from about 65,600 in 1999 to 89,000 in 2000.[3] A second agency reported that its 7 year fraud alerts increased about 53 percent in recent comparative 12-month periods; that is, the number increased from 19,347 during one 12-month period (July 1999 through June 2000) to 29,593 during the more recent period (July 2000 through June 2001). The third agency reported about 92,000 fraud alerts for 2000 but was unable to provide information for any earlier year.[4]

---

[1] U.S. General Accounting Office, *Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited*, GAO/GGD–98–100BR (Washington, D.C.: May 1, 1998).

[2] Public Law 105–318 (1998). The relevant section of this legislation is codified at 18 U.S.C. § 1028(a)(7)("fraud and related activity in connection with identification documents and information").

[3] These estimates are approximations based on the judgment and experience of agency officials.

[4] An aggregate figure totaling the number of fraud alerts reported by the three consumer reporting agencies may be misleading, given the likelihood that many consumers may have contacted more than one agency. During our review, we noted that various Web sites including those of two of the three national consumer reporting agencies, as well as the FTC's Web site, advise individuals who believe they are the victimes of identity theft or fraud to contact all three national consumer reporting agencies.

FTC: AN INCREASING NUMBER OF CALLS TO THE IDENTITY THEFT DATA CLEARINGHOUSE

The Identity Theft Act requires the FTC to "log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief" that one or more of their means of identification have been assumed, stolen, or otherwise unlawfully acquired. In response to this requirement, in November 1999, FTC established the Identity Theft Data Clearinghouse (FTC Clearinghouse) to gather information from any consumer who wishes to file a complaint or pose an inquiry concerning identity theft.[5] In November 1999, the first month of operation, the FTC Clearinghouse responded to an average of 445 calls per week. By March 2001, the average number of calls answered had increased to over 2,000 per week. In December 2001, the weekly average was about 3,000 answered calls.

At a congressional hearing in September 2000, an FTC official testified that Clearinghouse data demonstrate that identity theft is a "serious and growing problem."[6] More recently, during our review, FTC staff cautioned that the trend of increased calls to FTC perhaps could be attributed to a number of factors, including increased consumer awareness, and may not necessarily be attributed to an increase in the incidence of identity theft.

SSA/OIG: AN INCREASING NUMBER OF FRAUD HOTLINE ALLEGATIONS

SSA/OIG operates a fraud hotline to receive allegations of fraud, waste, and abuse. In recent years, SSA/OIG has reported a substantial increase in calls related to identity theft. For example, allegations involving SSN misuse increased more than fivefold, from about 11,000 in fiscal year 1998 to about 65,000 in fiscal year 2001. However, the increased number of allegations may be due partly to additional fraud hotline staffing, which increased from 11 to over 50 personnel during this period. SSA/OIG officials attributed the trend in allegations partly to a greater incidence of identity theft. Also, irrespective of staffing levels, a review performed by SSA/OIG of a sample of 400 allegations of SSN misuse indicated that up to 81 percent of all allegations of SSN misuse related directly to identity theft.

FEDERAL LAW ENFORCEMENT: INCREASING INDICATIONS OF IDENTITY THEFT-RELATED CRIME

Although federal law enforcement agencies do not have information systems that specifically track identity theft cases, the agencies provided us with case statistics for identity theft-related crimes. Regarding bank fraud, for instance, the FBI reported that its arrests increased from 579 in 1998 to 645 in 2000 and was even higher (691) in 1999. The Secret Service reported that, for recent years, it has redirected its identity theft-related efforts to focus on high-dollar, community-impact cases. Thus, even though the total number of identity theft-related cases closed by the Secret Service decreased from 8,498 in fiscal year 1998 to 7,071 in 2000, the amount of fraud losses prevented in these cases increased from a reported average of $73,382 in 1998 to an average of $217,696 in 2000.[7] IRS reported on the extent of questionable refund schemes involving a "high frequency" of identity fraud, that is, cases very likely to have elements of identity fraud. Regarding such cases, for a 5-year period (calendar years 1996 to 2000), IRS reporting detecting fraudulent refund claims totaling $1.76 billion and that 83 percent ($1.47 billion) of this total occurred in 1999 and 2000. The Postal Inspection Service, in its fiscal year 2000 annual report, noted that identity theft is a growing trend and that the agency's investigations of such crime had "increased by 67 percent since last year."

---

[5] On November 1, 1999, FTC established a toll-free telephone hotline (1–877–ID–THEFT) for consumers to report identity theft. Information from complainants is accumulated in a central database (the Identity Theft Data Clearinghouse) for use as an aid in law enforcement and prevention of identity theft.

[6] FTC, prepared statement on "Identity Theft," hearing before the Committee on Banking and Financial Services, U.S. House of Representatives (Sept. 13, 2000).

[7] In compiling case statistics, the Secret Service defined "identity theft" as any case related to the investigation of false, fraudulent, or counterfeit identification; stolen, counterfeit, or altered checks or Treasury securities; stolen altered, or counterfeit credits cards; or financial institution fraud.

COST OF IDENTITY THEFT TO THE FINANCIAL SERVICES INDUSTRY

We found no comprehensive estimates of the cost of identity theft to the financial services industry.[8] Some data on identity theft-related losses such as direct fraud losses reported by the American Banking Association (ABA) and payment card associations indicated increasing costs. Other data, such as staffing of the fraud departments of banks and consumer reporting agencies, presented a mixed and, in some instances, incomplete picture. For example, one consumer reporting agency reported that staffing of its fraud department had doubled in recent years, whereas another agency reported relatively constant staffing levels. Furthermore, despite concerns about security and privacy, the use of e-commerce has grown steadily in recent years. Such growth may indicate greater consumer confidence but may also have resulted from an increase in the number of people who have access to Internet technology.

Regarding direct fraud losses, in its 2000 bank industry survey on check fraud, the ABA reported that total check fraud-related losses against commercial bank accounts considering both actual losses ($679 million) and loss avoidance ($1.5 billion) reached an estimated $2.2 billion in 1999, which was twice the amount in 1997.[9] Regarding actual losses, the report noted that the 1999 figure ($679 million) was up almost 33 percent from the 1997 estimate ($512 million). However, not all check fraud-related losses were attributed to identity theft, which the ABA defined as account takeovers (or true name fraud). Rather, the ABA reported that, of the total check fraud-related losses in 1999, the percentages attributable to identity theft ranged from 56 percent for community banks (assets under $500 million) to 5 percent for superregional/money center banks (assets of $50 billion or more) and the average for all banks was 29 percent.

The two major payment card associations, MasterCard and Visa, use very similar (although not identical) definitions regarding which categories of fraud constitute identity theft. Generally, the associations consider identity theft to consist of two fraud categories account takeovers and fraudulent applications.[10] On the basis of these two categories, the associations' aggregated identity theft-related losses from domestic (U.S. operations) rose from $79.9 million in 1996 to $114.3 million in 2000, an increase of about 43 percent. The associations' definitions of identity theft-related fraud are relatively narrow, in the view of law enforcement, which considers identity theft as encompassing virtually all categories of payment card fraud. Under this broader definition, the associations' total fraud losses from domestic operations rose from about $760 million in 1996 to about $1.1 billion in 2000, an increase of about 45 percent. However, according to the associations, the annual total fraud losses represented about 1/10th of 1 percent or less of U.S. member banks' annual sales volume during 1996 through 2000.

Regarding staffing and cost of fraud departments, in its 2000 bank industry survey on check fraud, the ABA reported that the amount of resources that banks devoted to check fraud prevention, detection, investigation, and prosecution varied according to bank size. For check fraud-related operating expenses (not including actual losses) in 1999, the ABA reported that over two-thirds of the 446 community banks that responded to the survey each spent less than $10,000, and about one-fourth of the 11 responding superregional/money center banks each spent $10 million or more for such expenses.

One national consumer reporting agency told us that staffing of its Fraud Victim Assistance Department doubled in recent years, increasing from 50 individuals in 1997 to 103 in 2001. The total cost of the department was reported to be $4.3 million for 2000. Although not as specific, a second agency reported that the cost of its fraud assistance staffing was "several million dollars." And, the third consumer reporting agency said that the number of fraud operators in its Consumer Services Center had increased in the 1990s but has remained relatively constant at about 30 to 50 individuals since 1997.

Regarding consumer confidence in online commerce, despite concerns about security and privacy, the use of e-commerce by consumers has steadily grown. For exam-

---

[8] Generally, regarding the financial services industry, the scope of our work focused primarily on abstaining information from banks, two payment card associations (MasterCard and Visa), and the three national consumer reporting agencies.

[9] ABA, *Deposit Account Fraud Survey Report 2000*. The ABA defined "loss avoidance" as the amount of losses avoided as a result of the banks' prevention systems and procedures. Because the overall response rate by banks to the survey was only 11 percent, the ABA's data should be interpreted with caution.

[10] Other fraud categories that the associations do not consider to be identity-theft related include, for example, lost and stolen cards, never-received cards, counterfeit cards, and mail order/telephone order fraud.

ple, in the 2000 holiday season, consumers spent an estimated $10.8 billion online, which represented more than a 50 percent increase over the $7 billion spent during the 1999 holiday season. Further, in 1995, only one bank had a Web Site capable of processing financial transactions; but, by 2000, a total of 1,850 banks and thrifts had Web sites capable of processing financial transactions.[11]

The growth in e-commerce could indicate greater consumer confidence but could also result from the increasing number of people who have access to and are becoming familiar with Internet technology. According to an October 2000 Department of Commerce report, Internet users comprised about 44 percent (approximately 116 million people) of the U.S. population in August 2000. This was an increase of about 38 percent from 20 months prior.[12] According to Commerce's report, the fastest growing online activity among Internet users was online shopping and bill payment, which grew at a rate of 52 percent in 20 months.

COST OF IDENTITY THEFT TO VICTIMS

Identity theft can cause substantial harm to the lives of individual citizens potentially severe emotional or other nonmonetary harm, as well as economic harm. Even though financial institutions may not hold victims liable for fraudulent debts, victims nonetheless often feel "personally violated" and have reported spending significant amounts of time trying to resolve the problems caused by identity theft problems such as bounced checks, loan denials, credit card application rejections, and debt collection harassment. For the 23-month period from its establishment in November 1999 through September 2001, the FTC Identity Theft Data Clearinghouse received 94,100 complaints from victims, including 16,781 identity theft complaints contributed by SSA/OIG. The leading types of nonmonetary harm cited by consumers were "denied credit or other financial services (mentioned in over 7,000 complaints) and "time lost to resolve problems" (mentioned in about 3,500 complaints). Also, in nearly 1,300 complaints, identity theft victims alleged that they had been subjected to "criminal investigation, arrest, or conviction." Regarding monetary harm, FTC Clearinghouse data for the 23-month period indicated that 2,633 victims reported dollar amounts as having been lost or paid as out-of-pocket expenses as a result of identity theft. Of these 2,633 complaints, 207 each alleged losses above $5,000; another 203 each alleged losses above $10,000.

From its database of identity theft victims, after obtaining the individuals' consent, FTC provided us with the names and telephone numbers of 10 victims. We contacted the victims to obtain an understanding of their experiences. In addition to the types of harm mentioned above, several of the victims expressed to us feelings of "invaded privacy" and "continuing trauma." In particular, such "lack of closure" was cited when elements of the crime involved more than one jurisdiction and/or if the victim had no awareness of any arrest being made. Some victims told us of filing police reports in their home state but not being able to do so in the states where the perpetrators committed fraudulent activities using the stolen identities. Only 2 of the 10 victims told us they were aware that the perpetrator had been arrested.

In a May 2000 report, two nonprofit advocacy entities the California Public Interest Research Group (CALPIRG) and the Privacy Rights Clearinghouse presented findings based on a survey (conducted in spring 2000) of 66 identity theft victims who had contacted these organizations.[13] According to the report, the victims spent 175 hours, on average, actively trying to resolve their identity theft-related problems.

Also, not counting legal fees, most victims estimated spending $100 for out-of-pocket costs. The May 2000 report stated that these finding may not be representative of the plight of all victims. Rather, the report noted that the findings should be viewed as "preliminary and representative only of those victims who have contacted our organizations for further assistance (other victims may have had simpler cases resolved with only a few calls and felt no need to make further inquiries)."

Later, at a national conference, the Director of Privacy Rights Clearinghouse expanded on the results of the May 2000 report. For instance, regarding the 66 victims surveyed, the Director noted that one in six (about 15 percent) said that they

---

[11] Federal Deposit Insurance Corporation, *Evolving Financial Products, Services, and Delivery Systems (Washington, D.C.). (Feb. 14, 2001).*

[12] Department of Commerce, *Falling Through the Net: Toward Digital Inclusion* (Oct. 2000). This report was the fourth in a series of studies issued by Commerce on the technological growth of U.S. Households and individuals.

[13] CALPRIG (Sacramento, CA) and Privacy Rights Clearinghouse (San Diego, CA), "Nowhere to Turn: Victims Speak Out on Identity Theft" (May 2000).

had been the subject of a criminal record because of the actions of an impostor.[14] Further, the Director provided additional comments substantially as follows:

- Unlike checking for credit report inaccuracies, there is no easy way for consumers to determine if they have become the subject of a criminal record.
- Indeed, victims of identity theft may not discover that they have been burdened with a criminal record until, for example, they are stopped for a traffic violation and are then arrested because the officer's checking of the driver's license number indicated that an arrest warrant was outstanding.

FEDERAL CRIMINAL JUSTICE SYSTEM COSTS

Regarding identity theft and any other type of crime, the federal criminal justice system incurs costs associated with investigation, prosecutions, incarceration, and community supervision.[15] Generally, we found that federal agencies do not separately maintain statistics on the person hours, portions of salary, or other distinct costs that are specifically attributable to cases involving identity theft. As an alternative, some of the agencies provided us with average cost estimates based, for example, on work year counts for white-collar crime cases a category that covers financial crimes, including identity theft.

In response to our request, the FBI estimated that the average cost to investigate white-collar crimes handled by the agency's white-collar crime program was approximately $20,000 during fiscal years 1998 to 2000, based on budget and workload data for the 3 years. However, an FBI official cautioned that the average cost figure has no practical significance because it does not capture the wide variance in the scope and costs of white-collar crime investigations. Also, the official cautioned that while identity theft is frequently an element of bank fraud, wire fraud, and other types of white-collar or financial crimes some cases (including some high-cost cases) do not involve elements of identity theft.

Similarly, Secret Service officials in responding to our request for an estimate of the average cost of investigating financial crimes that included identity theft as a component said that cases vary so much in their makeup that to put a figure on average cost is not meaningful. SSA/OIG officials responded that the agency's information systems do not record time spent by function to permit making an accurate estimate of what it costs the OIG to investigate cases of SSN misuse.

Regarding prosecutions, in fiscal year 2000, federal prosecutors handled approximately 13,700 white- collar crime cases, at an estimated average cost of about $11,400 per case, according to EOUSA. The total cases included those that were closed in the year, those that were opened in the year, and those that were still pending at year end. EOUSA noted that the $11,400 figure was an estimate and that the actual cost could be higher or lower.

According to Bureau of Prisons (BOP) officials, federal offenders convicted of white-collar crimes generally are incarcerated in minimum-security facilities. For fiscal year 2000, the officials said that the cost of operating such facilities averaged about $17,400 per inmate.

After being released from BOP custody, offenders are typically supervised in the community by federal probation officers for a period of 3 to 5 years. For fiscal year 2000, according to the Administrative Office of the United States Courts, the cost of community supervision averaged about $2,900 per offender which is an average for "regular supervision" without special conditions, such as community service, electronic monitoring, or substance abuse treatment.

OBSERVATIONS ON IDENTITY THEFT AND LEGISLATIVE PROPOSALS

Given indications that the prevalence and cost of identity theft have increased in recent years, most observers agree that such crime is serious and warrants continued attention from law enforcement, industry, and consumers. Since our May 1998 report, various actions particularly passage of federal and state statutes have been taken to address identity theft. A current focus for policymakers and criminal justice administrators is to ensure that relevant legislation is effectively enforced. Along these lines, we identified several initiatives including coordinating commit-

---

[14] Beth Givens, Director, Privacy Rights Clearinghouse, "Identity Theft: Growing Problem of Wrongful Criminal Records," paper presented at the SEARCH National Conference on Privacy, Technology and Criminal Justices Information, Washington, D.C. (June 2000).

[15] As agreed with the requesters, our study focused on the costs of identify theft to the federal government only and not to state or local governmental entities; although, since 1998, most states have enacted laws that criminalize identity theft.

tees, multi jurisdictional task forces, and information clearinghouses that might help define the dimensions of the problem and help focus limited enforcement resources.

Moreover, there is general agreement that, in addition to investigating and prosecuting violations of these laws, a multi pronged approach to combating identity theft must include prevention efforts, such as limiting access to personal information. As you know, at the request of this Subcommittee and others, we have ongoing work looking at government agencies' use of SSNs and whether better safeguards or protections are needed. Prevention efforts can be particularly important, given the personal toll that this crime seems to exact on its victims and how difficult it is to investigate and prosecute perpetrators.

Although the scope of our work for today's testimony did not include an evaluation of various legislative proposals designed to combat identity theft, we did compile information that offers perspectives on various provisions of S. 1055 that are designed to address some aspects of the crime. For example, a major component of identity theft is acquiring personal identifiers such as SSNs, which are used in some states as driver's license numbers to build false identities. According to a 1999 study by the U.S. Sentencing Commission,[16] driver's licenses and SSNs are two of the most commonly misused identification means. In fact, the Commission's study reported that driver's licenses and SSNs are the identification means most frequently used to generate or "breed" other fraudulent identifiers. A provision (title II, section 205) of S. 1055 would prohibit the use of SSNs on driver's licenses or motor vehicle registration documents. In 1992, California enacted a law specifying that the SSN collected on a driver's license application shall not be displayed on the driver's license, including any magnetic tape or strip used to store data on the license. More recently, in November 2001, Ohio passed a law prohibiting the display of an SSN on a person's driver's license unless the person requests that the number be displayed. According to the American Association of Motor Vehicle Administrators, most states either prohibit display of the SSN on the face of the license or give the applicant the option to choose whether to display it.

Another potential source of personal identifiers for identity thieves is the personal financial information sold by financial institutions to non-affiliated third parties. The Gramm-Leach-Bliley Act of 1999[17] (GLBA) established the "opt-out" standard currently in effect. That is, unless an exception applies under the current standard, a financial institution must give consumers notice and the opportunity to opt-out before the financial institution can disclose private financial information to non-affiliated third parties. Generally, to implement the opt-out standard, financial institutions are required by law to send consumers an opt-out notice informing them of their right to prohibit its disclosure. In addition, financial institutions have to provide consumers an initial notice and customers an annual notice to inform them of the institution's information policies and practices. These requirements for federally regulated financial institutions became effective July 1, 2001. Limited data are available about the response to and effectiveness of such notices. However, another provision (title III, section 302) of S. 1055 would impose a stricter standard if the financial institution seeks to sell the information. Specifically, that provision would amend GLBA to provide consumers an "opt-in" standard, whereby a bank would need prior consent of the customers before selling personal financial information to non-affiliated third parties.

Resource levels and competing priorities can limit any one level of government's capacity, including the federal government's capacity, to address identity theft crimes. Another provision (title VI, section 601) of S. 1055 would empower state attorneys general to enforce this act. Regarding precedent for such a provision, although GLBA does not have a similar provision, the act's legislative history indicates that earlier versions of the House and Senate bills included similar state enforcement authority, which was dropped in conference. In further reference to precedent, however, one example of an enacted provision is in the antitrust context. State attorneys general have the authority to bring civil actions on behalf of resident consumers who have been injured as a result of violations of federal antitrust laws.

In a similar vein, resource constraints and dollar threshold levels have limited the numbers and types of cases that federal law enforcement agencies have investigated. One type of case that has not often been investigated involves SSN misuse. Currently, SSA/OIG devotes its investigative resources to program integrity priority areas rather than SSN misuse cases. SSN misuse allegations increased more than fivefold, from about 11,000 in fiscal year 1998 to about 65,000 in fiscal year 2001.

---

[16] U.S. Sentencing Commissions, *Identity Theft Final Report* (Washington, D.C.) (Dec. 15, 1999)

[17] Public Law 106–102 (1999).

Title II, section 207 of S. 1055 would give SSA the authority to impose civil monetary penalties for SSN misuse. It is not clear how the SSA/OIG would carry out this new authority or how many additional resources it would require and at what cost.

In sum, while legislative and other actions have been taken in recent years to address identity theft, incidence and cost data indicate that more can and should be done. The provisions contained in S. 1055 and other proposed legislation are aimed at enhancing the prevention and enforcement tools available to law enforcement, industry, and consumers. These legislative proposals deserve careful attention and analysis.

Madam Chairwoman, this concludes my prepared statement. I would be pleased to answer any questions that you or other members of the subcommittee may have.

CONTACTS AND ACKNOWLEDGMENTS

For further information regarding this testimony, please contact Richard M. Stana at (202) 512–8777 or Danny R. Burton at (214) 777–5600. Individuals making key contributions to this testimony included David P. Alexander, Shirley A. Jones, Robert J. Rivas, and Ronald J. Salo.

Chairperson FEINSTEIN. Thank you very much. I think it is fair to say that we have got a substantial and rising problem in the United States. I mean, some law enforcement people have told me that it is the single largest rising crime in America. Would you agree with that?

Mr. STANA. I do not know if it is the single largest crime, but I cannot think of one that is rising faster. It is touching every facet of our society. It is touching victims, it is touching businesses, it is touching government, and from that standpoint alone, it suggests that more needs to be done.

Chairperson FEINSTEIN. I have also been told that the burden of proof is really on the victim, who has to go and reestablish their identity, and that the average length of time that it takes a victim to reestablish their identity is 18 months. Did you do any work in that area?

Mr. STANA. We phoned ten victims that were identified through the FTC's data clearinghouse and asked them a number of things, like the impact of their victimization, how long it took them to unwind their case, and some of the impacts that they received from being a victim. They told us, on average—of course, there were some at the low end, some at the high end—but about 150 to 200 hours it took them of their personal time to unwind the case.

Oftentimes, they did not lose financially as much as they just lost their ability to get car loans. Interestingly, in four cases we identified, the identity theft victim actually went to jail for some time while they were trying to unwind their identity.

I might also mention, Senator, that one interesting facet of this is about three-quarters of the victims have no idea how their identity was stolen. They do not know if it came from somebody who stole mail. They do not know if it came from the Internet. They do not know if it came from a huge data base. But the 25 percent who did know, about half of those found that it was somebody who they have a personal relationship with, a friend, a co-worker, somebody down the street who stole their identity.

Chairperson FEINSTEIN. I am told that the two major centers for identity theft are Los Angeles and Oakland, California, interestingly enough, and some of the testimony that I have received indicates that, often, obituary columns are good sources of information that lead to the theft of identity because mother's name, father's name are listed there, and then the individual has a basis to go out

and get access to the Social Security number or the driver's license and they can also look up the financial data, buy the financial data of the individual.

I am particularly aware of one case where, I think it was the No. 2 executive at the Cedars of Lebanon Hospital in Los Angeles, he passed away and the obituary was in the Los Angeles Times. His widow was essentially bilked of, I think, $300,000 by identity thieves who got what they needed to get the documents right out of the obituary column. Have you encountered anything like that in your examination?

Mr. STANA. Well, the key pieces of information that are used to create an identity, a false identity, are the names, address, Social Security number, date of birth, and mother's maiden name, and if you can get a combination of those from various sources, if you have some from an obituary, for example, a mother's maiden name and the name and the address, and go into some research engine on the Internet and pull down other information, you can easily build a new identity.

This really underscores two things. Not only do we need to pay attention to the law enforcement needs related to identity theft, but the prevention needs are tremendous. I know you addressed some of them in S. 1055, but the need for individuals to protect their personal identifiers like they would protect their wallet or their purse is just so important. It cannot be understated.

Chairperson FEINSTEIN. Mr. Stana, I must go to the vote, so we will take a brief recess. If you would not mind staying, Senator Cantwell is going to be here following the vote and she has indicated that she has some questions she would like to ask. So if you do not mind———

Mr. STANA. Not at all.

Chairperson FEINSTEIN. and everybody else does not mind, we will take a brief 10-minute, strict 10-minute, recess.

[Recess.]

Chairperson FEINSTEIN. We will reconvene, and thank you very much for your forbearance.

I am delighted to be joined by the Ranking Member. He and I have worked very closely on this committee now for a number of years, and speaking for myself, I find it most enjoyable to work with him. Mr. Stana, if it is all right with you, I will defer to the Ranking Member now for his comments.

STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KYL. Thank you, Senator Feinstein. I am not going to read my entire opening statement. I will ask that be put in the record. I welcome all of the witnesses. I am sorry I missed Senator Gregg.

Senator Feinstein is absolutely right. We have worked on this particular problem for many years now together, and probably nothing has been more frustrating to either one of us than the inability to stop this kind of crime. We can diminish it. We can help the people who have been victims of the crime, although we are clearly not doing enough to do that. And I guess one of the biggest frustrations I have and one of the things that makes me most hum-

ble, in other words, to demonstrate that will all of the great power we are supposed to have, we still cannot get this problem solved. It is a very difficult thing and it bothers me a great deal.

I just have a couple of questions to ask of you. I appreciate your testimony. We reviewed that. My apologies for not being here right at the very beginning. Senator Feinstein probably said we have a lot of different commitments. This week, for the first time ever, all four of my major committees held hearings at exactly the same time on the same day. It is a little hard to be in all four places at the same time.

Chairperson FEINSTEIN. Thanks very much, Senator. I am glad you are here.

[The prepared statement of Senator Kyl follows:]

STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Thank you Senator Feinstein for convening this important hearing on the issues of privacy, identity theft, the protection of our personal information. I am very aware of the American public's continuing concern about the collection and the distribution of personal information. For several years Senator Feinstein and I have worked to prevent criminals from gaining access to a citizen's personal information to commit identity crimes. In 1998, Congress passed the Identity Theft and Assumption Deterrence Act which increased protection for the victims of identity theft. I am very proud that I was able to introduce that particular piece of legislation; however, I realize that we need to do more.

Identity theft is escalating at an alarming rate. It is a crime that is not limited to a particular age, gender, economic, or racial group, but instead is found in all parts of our society. The Federal Trade Commission reports that it has processed over 97,000 entries from consumers and victims regarding identity theft, as of June 2001. I am eager for today's witnesses to fill us in on the details, and update us on the severity of the problem we are facing. I also look forward to their suggestions about where best we can direct our efforts to protect our citizens.

The collection of and retention of an individual's personal, financial, and health information has become a highly profitable industry in today's e-commerce. An entire industry has arisen that operates solely for the purpose of collecting and brokering private information. This information is a valuable commodity for companies in today's competitive consumer marketplace and these industries with their vast databases should protect the information they contain.

It is also important to note, at this time, that this collection of information is beneficial to consumers. They are offered products that are tailored to their specific needs; companies are forced to be more competitive; and the exchange of information facilitates the growth of our economy. Therefore, we must carefully balance the restrictions we place on business. An overly restrictive standard could harm the nation's economic health. Online retail sales have jumped 67% from the fourth quarter of 1999 to the fourth quarter of 2000. Retail sales at the end of 2001 totaled approximately 104 billion dollars. It is clear that the public, in increasing numbers, continues to have confidence in the Internet for the purchase of goods and services.

It is the responsibility of the private sector, government, and consumers to lessen likelihood of this private information will fall into the wrong hands. It is a common misconception that the increase in identity fraud and identity theft is caused by the Internet. Although, e-mail scams and attacks by hackers are increasing, the FTC reports that the two most common causes of identity theft are, lost or stolen purses and wallets, and mail theft. Also, that the majority of identity- theft crimes are committed by individuals we personally know—for example, family members, friends, or coworkers.

Identity theft is a crime that affects all Americans and encompasses many different types of fraud. The Federal Trade Commission's Identity Theft Hotline reports that:

- about 43% of complaints involved credit-card fraud
- about 21% of complaints involved activation of telephone, cellular, or other utility service in the victim's name
- about 14% of complaints involved bank accounts that have been opened in their name, and/or fraudulent checks have been negotiated in the victim's name

- 7% of complaints involved consumer loans or mortgages that were obtained in the victim's name
- 7% of the victims reported that identity the identity thief had obtained or forged a government document, filed a fraudulent document, or obtained government benefits under their name.

One major area of personal information is personnel medical records. Access to these records is an extremely sensitive issue facing Congress. Medical technology is advancing at an exponential rate. Medical professionals will be able access a patient's medical history; even his or her genetic profile will be accessible to potentially arrive at better and more accurate treatments. However, there is a concern that this data could be used to deny an individual medical insurance, employment, or even a mortgage. Even the use for marketing purposes, without an individual's permission, is extremely intrusive.

Senator Feinstein, you have assembled what promises to be a very interesting and informative group of witnesses here today. I look forward to their testimony and delving into their privacy concerns and recommendations. I would like to extend my thanks for the time they have taken to assist this Subcommittee in grappling with some very complex issues that will touch the lives of many Americans.

In closing, I look forwarding to working with my esteemed colleague from California, who has always shared my concern about identity theft and the protection of our citizens' privacy.

Chairperson FEINSTEIN. I am pleased to welcome Senator Cantwell. If you have a comment, Senator, or would you like to make a statement?

STATEMENT OF HON. MARIA CANTWELL, A U.S. SENATOR FROM THE STATE OF WASHINGTON

Senator CANTWELL. Yes. Thank you, Senator Feinstein. I will be brief and add a longer statement to the record, but I particularly wanted to thank you and Senator Kyl for your leadership on this important issue, actually both issues of consumer privacy and the issue of identity theft. I am particularly pleased that we are going to hear from the General Accounting Office who are going to give us some concrete data about the growing problem of identity theft.

I have introduced a bill that will be considered in this subcommittee giving victims of identity theft greater tools to recover their identity and restore their good credit and I appreciate, too, that Senators Feinstein and Kyl have a bill that will enhance identity theft prevention which will also be considered.

These are very critical issues and a growing problem and I appreciate the committee's attention to them. Thank you.

Chairperson FEINSTEIN. Thanks very much, Senator.

[The prepared statement of Senator Cantwell follows:]

STATEMENT OF HON. MARIA CANTWELL, A U.S. SENATOR FROM THE STATE OF WASHINGTON

I want to thank Chairwoman Feinstein for holding this hearing. Particularly, I want to thank her, and Senator Kyl for their leadership on the extraordinarily important issues of consumer privacy and identity theft.

I am particularly pleased that we have the General Accounting Office here today to give us some good data about the growth and cost of identity theft. I have introduced a bill that we will be considering in a few weeks in this Subcommittee that will give victims of identity theft the tools to recover their identity and restore their good credit. I appreciate too, that Senators Feinstein and Kyl have a bill that will enhance identity theft prevention, which we will also consider. These are critical issues, and as we will hear, it is a problem growing at an unprecedented rate.

Let me turn to the broader issues of consumer privacy. Consumer privacy is a complex issue: with the rapidly changing capabilities of new technologies, and information being collected by a wide range of entities, I see this as an urgent matter. As new technologies are developed, new uses of personal information continue to

arise. Many will prove a great benefit to consumers, but all will come with the concern that privacy be protected. We are only at the tip of the iceberg on these issues.

I think a lot of people are asking the right questions: The first question has to be "what are consumer expectations in regard to their privacy?"

Consumers and businesses alike need clear, recognizable 'rules of the road' for privacy. Privacy law needs to be as clear to everyone as the basic rules of driving—you know to drive to the right of the center divider, you know to stop at the red hexagon—and you know to yield to a crossing pedestrian.

For me, the bottom line is that we need a federal legal framework so consumers know their privacy protections and businesses know how to handle a consumer's information. So expectations can be met. I look forward to continuing to work with the members of this Committee and others in Congress to enact the appropriate protections for the good of the consumer and the good of the economy.

Again, thank you Madam Chairwoman and I look forward to hearing the testimony today.

Chairperson FEINSTEIN. I have two more quick questions and then I will turn to the Ranking Member. Mr. Stana, how many Social Security number misuse cases are being investigated by the Social Security Administration Office of the IG?

Mr. STANA. The short answer is, less than 2 percent of the allegations that are given to the Social Security IG are investigated.

Chairperson FEINSTEIN. Why is that?

Mr. STANA. Well, it boils down to three things, really. It is threshold, priorities, and resources. Oftentimes, these allegations involve small amounts of money, or one case as opposed to a ring, and so it gets pushed off for threshold reasons.

Priority, the Social Security IG focuses more on program fraud rather than misuse fraud, so these cases fall through the cracks. The fact is, they are falling into a hole. Nobody is investigating them.

And the third reason is there just are not enough resources to do the whole job.

Chairperson FEINSTEIN. Is the same true for the FTC?

Mr. STANA. It is interesting. You are bringing up a good point. The infrastructure has been created by the 1998 Act that I know you all have helped to enact into law, and we have the FTC creating a clearinghouse of data. More and more calls are coming in each week, so the public is beginning to become aware of the potential for having this data in a central place.

The fact of the matter is, we built a library that not many people are coming to to check out books. There is only one part-time Secret Service agent that is going there to mine the data. Nobody else is using it.

Similarly, task forces are being created around the country to combat white collar crime and part of that is identity fraud as one of the crimes. But there is not as much action in those task forces related to identity theft that the growth in this crime would suggest needs to be.

Chairperson FEINSTEIN. Thank you. I am hopeful that this bill will be able to set the kind of basis for greater attention to it.

Senator Kyl?

Senator KYL. Thank you, Madam Chairman.

With regard to that last question, it is interesting, and one thing I have been kind of curious about is whether, after we passed the law, you could identify any change in the statistics or the behavior in terms of quantification. Have you been able to factor in, as a result of greater public awareness or we hope greater public aware-

ness, have you been able to factor in any effect of that in the crimes reported or the incidences of theft?

Mr. STANA. The number of crimes reported to the FTC has increased from about 450 in 1999 when they set up the clearinghouse to about 3,000 a week now. So you can see that the public is becoming aware of the FTC being one shop to call to report identity theft.

The other side of that, though, is that not much seems to be made of that data. There is some data mining going on by one Secret Service agent to try to identify trends and put together rings to help investigate the crime, but not much more than that.

Senator KYL. One thing at least that I had hoped we would do is to create some kind of a matrix, which is probably the wrong word, but a profile, in effect. Do you have any idea whether work has been done to determine whether the bulk of this is just single-shot criminals, whether it is terrorists, whether it is organized crime or what the matrix of the people committing this fraud looks like?

Mr. STANA. Well, we know some data and we know some information about this crime. For example, most victims are of a certain age. Thirty, I think, is the average age. I think 75 percent fall between 18 and 59. Ron, do you have other information that you might share with us?

Mr. SALO. Regarding the specific question you had, who are these perpetrators, there is no data out there to tell us whether the majority are organized crime rings, ethnic groups, or whether they are individuals operating as loaners. The problem in answering that question is you first need good information and then you need good analysis of that information. If the analysis is not being done, then individual victims who call in are not being analyzed in a way so that you can identify one perpetrator or gang that is actually victimizing many people who are calling in.

Senator KYL. You all may not be the best ones to answer this question, but obviously, given the fact that we found information tying terrorists to this crime as a way of funding some of their activities, A) has work been done to try to track that down and identify the size and scope of that problem, and B) do you know of anything that has been done to, in effect, isolate those particular cases?

Mr. SALO. We have one piece of information from the U.S. Sentencing Commission, a very excellent report on identity theft. It was performed before September 11 on conviction data from the courts, so we have solid information, and that report indicated that one out of three identity theft victim convictions was from a foreigner, not from an American citizen.

The distribution of countries that made up this sample of foreign convicted identity thieves is very long, mostly one from one country, one from another country. There were only two countries that seemed to be a little bit of a bubble, where there were more convictions, and that was, firstly, Mexico, and then Nigeria. After that, it was mostly one each. There was some distribution that indicated wide dispersion of countries being represented.

Senator KYL. Now, were these foreigners in the United States legally, or do you have any way of knowing that?

Mr. SALO. The information in the report did not reveal whether they were or not.

Mr. STANA. I might add, though, that INS has a tremendous problem dealing with illegal aliens using false identities to seek work authorization documents and so on. So I suspect, being most of them from Mexico and Nigeria, they were probably work-related rather than terrorist related.

Senator KYL. One of the questions we have had, too, relates to the disparity in the numbers between the reporting from credit bureaus and the like and your reporting. I did not know this number. This is what staff wrote down, that you indicated there were about 750,000 victims, I guess is what the number ties to. Could you repeat that for me again? I am sorry I was not here.

Mr. STANA. Let me clarify that. You could probably look at this as a very conservative figure, a mid-range figure, and a very high figure. I think the 750,000 would probably be at the upper end of victims. At the lower end, you would have a range of 250,000 to 300,000, and then a mid-range of 400,000 to 500,000, and it really depends which data you put into this estimate and what assumptions you make. The most conservative is the data available and things you can actually count rather than estimate, and that is the lower end, 250,000 to 300,000.

Senator KYL. My red light is on, but I do want to get into that in just a little bit more detail when we come back.

Chairperson FEINSTEIN. Thanks, Senator Kyl.

Senator Cantwell?

Senator CANTWELL. Thank you, Madam Chairman.

Mr. Stana, I know your report covers many things in looking at this from a perspective of how individuals are being impacted. Did you get a sense of how long the average identity theft investigation takes?

Mr. STANA. I do not have that information. I know that the identity theft victims take between 150 and 200 days to unwind their case, and I know that sometimes these cases can go on for months and months and months. I do not have an average figure.

Senator CANTWELL. But it is safe to say the maximum length of the investigation is quite some time?

Mr. STANA. It can be quite some time, and that is because these cases are not easy to investigate and it is because the financial transactions that are done illegally often are very intricate.

Senator CANTWELL. So that issue with the statute of limitations not occurring until—basically occurring at the time of the crime as opposed to the time that an individual finds out is a major issue?

Mr. STANA. Well, it is a major issue. Unlike so many other crimes, by the time the victim knows they have been victimized, it could be months later and the trail is cold.

Senator CANTWELL. I know that this was not the scope of your report, but through your research, did you get a sense of how many years after the fact that people are then burdened with this? I think some people think you might clean this up by making a few phone calls.

Mr. STANA. We were talking with a victim this morning, in fact, who told us that her identity was stolen and she did not know how, but 1 year after her identity was stolen, she was contacted by a col-

lection agency on a $22,000 cellular phone bill that she had no idea how it got there and it took many calls, much effort. She said it probably took in the neighborhood of 300 days to get this straightened out. Incidentally, at the time, she was purchasing a house and she was afraid that the adverse credit rating may sneak into that transaction, but fortunately, the credit bureaus had put the flag on things and straightened that out.

Senator CANTWELL. So you did not have any information about what kind of permanent or long-term damage to individuals' records might—

Mr. STANA. It is interesting. In some cases, there is long-term damage. In other cases, there is not. We came across four cases, and it was incredible to listen to the stories, but four cases where the person whose identity was stolen actually had to go to jail for some time for the crime until the crime was unwound.

Senator CANTWELL. One of the reasons why I introduced legislation was because there was someone in our State who had been convicted of a crime that they did not commit, either, because of identity theft.

In the process of gathering information for the study, did you get any sense of the percentage of identity theft crimes that are State or local investigations or prosecutions as opposed to Federal investigations, because obviously this is not exactly a crime that you call 911 about. Oftentimes, it is very confusing. I know that we have made some changes there and have a Federal agency involved with a number that people can call. But did you get any, if not empirical, just a sense of the magnitude of where the enforcement focus needs to be?

Mr. STANA. When a person's identity is stolen, they are supposed to do four things. First, they are supposed to call the credit bureaus to put a flag on their account. Then they are supposed to call the bank or the vendor and notify them that their identity is stolen. Third, they are supposed to call the local police department, not the Federal but the local police. And finally, they are supposed to call the FTC. So you are exactly right that this is more of a State and local than a national crime.

That being the case, despite our efforts, we could not locate any data which told us the extent of the crime, how much of it was federally reported and investigated, how much locally reported and investigated. But there is a frustration among people who do report locally and that is oftentimes local and State police departments are not well equipped to handle or to investigate this crime.

Senator CANTWELL. So that would be an important step in the next process, right?

Mr. STANA. Yes, I think it would, in enforcement. I think you have to separate what is needed into two buckets, what is needed from a prevention standpoint and what is needed from an enforcement standpoint, and certainly the State and locals factor heavily into what is needed from an enforcement standpoint.

Senator CANTWELL. Giving information to both the victims and to law enforcement at the local level.

Mr. STANA. Well, and having local police have an understanding of what to do with the allegation. I think they full well know how

to handle, say, a murder or how to handle traffic violations. How to handle a financial crime is often beyond their capability.

Senator CANTWELL. Did you hear—

Mr. STANA. Another factor there is, too, you may live in one jurisdiction and the crime is reported or happens in another jurisdiction and you get into jurisdictional boundary issues.

Senator CANTWELL. That is another thing that we try to address in my legislation.

I know my time is in the yellow here, but I wanted to followup on that in the sense that local law enforcement and the individual victims need access to the information, and oftentimes, what I think you are saying verifies this, what happens is the victim finds out that something is amiss, calls the credit bureaus to flag something, but then no more information is given to them or to the crime unit to be able to prosecute or move on that identity theft.

Mr. STANA. What a victim of identity theft should be sure to do is every call that is made to a credit bureau or to the financial institution that may be carrying the card or the merchant is to ask them to forward to the victim whatever information they have available in their files, so that in the course of the investigation if other information is needed or information that the victim can supply would be helpful, they would have that information at hand.

Senator CANTWELL. Well, I think what happens oftentimes is calling some of these people that, I think, have been a victim of any theft, they are not sure who is now the victim. Is it the person that is calling or the person that created the transaction? I know our State of Washington and other States have taken the measure to try to give a document to the person whose identity has been violated that they can use in communicating with law enforcement and others to verify that information. So an actual verification that they are, in fact, the victim and not somebody who is perpetrating a crime.

Mr. STANA. It would be useful to have a checklist for the victim. They can go down and say, yes, I contacted this, I asked for this document, they are going to help me, this office is going to do this. I ought to caution, though, that there is not much investigation going on with the credit bureaus on these individual allegations. So the kinds of information you are likely to get from a credit bureau or even from a credit card company or other financial institution is simply the date of a transaction, where the transaction was made, and for the amount. You probably would not get much of a description, if any, of the perpetrator.

Senator CANTWELL. Not at this point.

Mr. STANA. Not at this point, but those leads may be useful for law enforcement.

Senator CANTWELL. Thank you. I know my time is expired.

Chairperson FEINSTEIN. Thanks, Senator.

I would like to enter into the record the statement of Senator Hatch on this issue, without objection.

Senator Kyl, you had other questions?

Senator KYL. I just had one last question and then we want to get on to the next panel. I would like to have you help us resolve the discrepancy between the figures that you have come up with and figures from the credit industry. I think maybe the best way

to do that is you are probably aware of the figures they have, but we can give you that information and maybe just have you write us a note on what your analysis of that is and why the discrepancy and so on. But I would appreciate hearing anything you have to say right now.

Mr. STANA. We can quickly walk you through how we get to the low end, the mid-range, and the high end.

Senator KYL. Please do, and then if you would just also look at what their data is and drop us a note about why you think your data is more reflective of the correct situation than theirs, or whether theirs is, or whatever you have to say about it.

Mr. STANA. I think we would be more comfortable saying what the assumptions and the data were to get it to one level, the next level, and the next level.

Senator KYL. All right.

Mr. STANA. Given that the data is very uncertain and given that there is so much that is not recorded here, it is really hard to say that this is the correct level or that is the correct level.

Mr. SALO. As Mr. Stana is saying, the key to this whole discrepancy issue is the recognition that there is no one place to go to get a comprehensive statistic on the prevalence of identity theft. This was true 2 years ago when we were doing our work on identity theft. It is true today, even though there is an FTC Identity Theft Data Clearinghouse that is available to victims to call in.

To explain how we came up—

Senator KYL. Excuse me 1 second. In that clearinghouse, is there not a checklist? Senator Cantwell was right on in terms of a checklist, but is there not some kind of a checklist in that particular site, the FTC site?

Mr. SALO. There is, and as a matter of fact, the points—for example, on their webpage, the things that an identity theft victim should do are actually listed out on the webpage and Mr. Stana has already articulated those, basically the four points. We would certainly agree that those are the proper steps that any identity theft victim ought to take.

Senator KYL. OK, and one other thing. We have that on my Senate website and I think what we ought to do is maybe send a "Dear Colleague" to our colleagues and suggest that they put it on their own website or get it out any other way that would be useful to folks.

Mr. SALO. There are many ways to be useful, not to avoid the question. I will get exactly to your question. But one thing that we were looking at very recently was whether the Social Security Administration in their annual notices to people about their benefits has anything on identity theft and I was surprised to notice that on the very top of every notice, it says that this is an alert to be aware of a misuse of your Social Security number and there is a report that the Social Security Administration cites that you could get which, again, tells you how you can minimize the vulnerability you have to becoming an identity theft victim.

But coming back again to your original question, how do we come up with a number, given that we have a patchwork of sources, we looked at the credit bureaus and we looked at the FTC Data Clearinghouse and we looked at the Social Security Administration as

three early warning bells up front where prevalent statistics might be present.

We talked to the three national credit bureaus and asked them about the telephone hotline statistics that they have and they more or less came up with a consensus that we agreed with that a solid figure, a reliable figure would represent fraud alerts. Fraud alerts represent a notice on individuals' accounts, basically alerting anyone who is in a retail outlet who is receiving an application for new credit, that person would be alerted that perhaps this person is a potential victim to identity theft and let us call the person at home and make sure that this is, in fact, not the case.

Fraud alerts look like a good mechanism. The reason why they thought it would be reliable is because there are people who call in perhaps to get a free credit report and they may not, in fact, be a victim and it is a way of culling out—reducing the statistics down to a reliable number of people who definitely say, yes, I am an identity theft victim and I want a fraud alert on my account.

The only drawback of that is that the three credit bureaus have different business processes for getting to that 7-year—that is how long the fraud alerts are—seven-year fraud alert flag, and in the more complicated processes, you start to lose people as you call through. Our range was 30,000, approximately 30,000 to 178,000. One explanation for that disparity is the higher number represents the one-time call. The lower number represents two calls and additional documentation to be provided to the credit bureau.

Now, who are people calling credit bureaus? They are people who have either been harassed by a collection agency and been alerted that there is an expense that they were not aware of and they are afraid that it might be affecting their creditworthiness, or they may, in fact, get a bill that they do not recognize and they want to dispute it and, in fact, it may be because they were victimized.

But there is a third group out there of people who would rather be safe than sorry. This historically has always been part of the statistics built into the credit bureaus' reporting. In one credit bureau, that proportion of those who would rather be safe than sorry versus victims has grown over time from what used to be one out of three calls to now approximately one out of two calls. We regard that as an indication that the education and awareness of the consumer is finally getting out, that people recognize the risk of identity theft and they are calling in to put on fraud alerts because they would rather be safe than sorry.

However, not everyone does call a credit bureau. Consequently, we looked at the sources of data and asked ourselves, which ones appear not to be duplicative? Could we then add them up? and I can run down the list very quickly right now.

The FTC, based on the fact that they are telling us approximately 3,000 victims call in to their clearinghouse every week, if we were to annualize that, it would come out to about 150,000 victims. Additionally, the Social Security Administration's hotline, Office of Inspector General Hotline, receives SSN misuse allegations and those are, to a large degree, not the same people because there is a memorandum of understanding between the FTC and the SSA OIG to have that information shared. So the 56,000 calls now that

come into the—on SSN misuse could be added to the 150,000 from the FTC.

Chairperson FEINSTEIN. I would like to move on, if that is all right.

Senator KYL. Yes, please.

Chairperson FEINSTEIN. Gentlemen, I would like to move on, but thank you very much. I just want to add one thing for the record. For the 23-month period from its establishment in November 1999 to September 2001, the FTC Identity Theft Data Clearinghouse received 94,100 complaints. Of these, nearly 1,300 complaints, identity theft victims alleged they had been subject to criminal investigation, arrest, or conviction. So I would like the record to reflect that.

Thank you very much, gentlemen. We appreciate it.

If we could call the next panel, please. The next panel consists of Susan Fisher of the Doris Tate Crime Victims Bureau, Doug Comer of Intel, and John Avila of the Walt Disney Company.

Susan Fisher comes to us from my State, from Carlsbad, California. She is the Executive Director and Vice Chairwoman of the Doris Tate Crime Victims Bureau. In 1987, her brother was killed, as I said, by his ex-girlfriend who stalked him by obtaining his credit card information, phone records, and other personal information. Since her brother's murder, Susan has been a relentless advocate for victims' rights. Under her leadership, the Doris Tate Crime Victims Bureau has received the San Diego District Attorney's Award for Service to Crime Victims and she has twice been the recipient of a certificate of appreciation from the Department of Justice for service to victims of crime.

Susan Fisher, we welcome you, and if you would like to proceed. We are going to limit your statement to 5 minutes so we have some time for questions.

STATEMENT OF SUSAN FISHER, EXECUTIVE DIRECTOR, DORIS TATE CRIME VICTIMS BUREAU, CARLSBAD, CALIFORNIA

Ms. FISHER. I would like to talk about the crime of stalking in general and specifically use some examples from the case that I know best, which was my brother's murder.

Ron, my brother, was murdered after being stalked for over a year by Linda Ricchio, who was a former girlfriend who had become obsessed with him. They had actually stopped dating a few years before the stalking began, but he had had difficulty extricating himself from the relationship with Ricchio because his attempts to leave would always be followed by her manipulation of him with things like staged suicide attempts, public scenes that were meant to embarrass him, and threats of violence against his friends and family members, which are all very typical of stalkers.

From the moment that Ron ended their relationship, she began to access personal information about him in order to track his whereabouts and know who he talked to and who he spent time with. She was easily able to get copies of phone bills and utility bills. She was able to trace his fiancee and his fiancee's mother by accessing DMV information.

Since 1987 when that was happening, Congress has passed legislation to protect drivers' license information, but there are still

some loopholes in the current law and Senator Feinstein's bill would mandate that you give consent before your driver's license information could be sold and we feel that that is a very important piece of legislation to have in place.

In 1987, in my brother's case, Ricchio quit her job and stopped going to school in order to stalk my brother, Ron, on a full-time basis. She actually stalked him so relentlessly that she locked up her house, left her cats to die of starvation, and spent every day, all day, stalking him.

In November of that year, he was compelled to get a restraining order in order to try to protect himself and also to protect his job. The San Diego County judge who issued the restraining order at that time told him that he should be flattered by the attention. Obviously, the crime of stalking is getting a little more attention now and is being taken a little more seriously. After being told that he should be flattered by the attention and really kind of supporting her position in the case as just attention to an ex-boyfriend, Ricchio left the courthouse in San Marcus, California, legally bought a gun after having the restraining order filed against her.

In November, the daily contact stopped. We learned later that Ricchio had gone to San Francisco during that period to visit her brother and to enlist his help in developing over 200 surveillance photos that she had taken of my brother. During that time, my brother moved for the third time that year. He was trying to buy a little time, trying to decide what to do, and rapidly coming to the conclusion that there was really nothing that he could do if she decided to become violent. With her ability to track him down, he was convinced that even if he left the State, she would eventually find him using phone records or one of the other kinds of trails that we all just leave just by existing in this world.

On December 9, after once again tracing his whereabouts, she rented the apartment next door to him without his knowledge. The two-story apartments that he lived in were separated by—the two apartments, I beg your pardon, were separated by a privacy wall. Hers was at the back of the balcony and his was at the front.

On Monday evening on December 14, he came home from work. He had actually asked to come home a little bit late because it was getting dark early and his lights in his parking lot did not come on until about 5:30, so it was about 5:30 in the evening. He came up the stairs carrying a bag of groceries in his left arm and his checkbook and his keys in his right hand. He turned his back to the privacy wall, bent over to put the key in the door, and at that point, Ricchio stepped out from behind the wall and she fired a shot into his back. She shot him twice, once as he ran down the stairs away from her in the dark.

At the time that Ron was killed, there were no stalking laws in California. In fact, they did not even use the word "stalking." It was considered harassment or domestic violence. California was actually the first State to pass stalking legislation, and in the years since my brother's murder, I have been very involved in working on anti-stalking legislation in California and working directly with stalking victims. In fact, most stalking victims in many parts of California end up coming to the bureau for the very reason that we have done so much work on legislation on stalking.

While many things have changed, both in the criminal justice system and in the way that we view stalkers, since my brother was murdered in 1987, the pathology of stalking remains the same. We recently have seen an increased use of Internet venues, particularly by domestic violence-type stalkers, to contact and harass their victims. and while we have been able to legislate many safeguards into avenues of access that stalkers once used, new avenues are opening up all the time.

Stalkers who often are sociopathic and have borderline personalities have the intelligence and the drive necessary to access any information available in order to track their victim and would most certainly be willing to purchase the information. Information on the Internet that is not safeguarded is fair game.

I have a little bit of information here that I actually found on the airplane on my way here that talks about some websites that are out there now. There are websites such as one that is called "Spy for You" that sell unlisted phone numbers and bank account numbers and trace pager numbers to home addresses. There is a company called DBT Online, which would match a name with a Social Security number, date of birth, and telephone number for a small fee. Also, unprofessional private investigators would have very easy access to this kind of information through the Internet and many stalkers would be more than willing to pay them for that information.

We just feel that it is important to mandate the kind of protection that having to give permission for that information to be sold is very important and that is why I am here today. Thank you.

Chairperson FEINSTEIN. Thanks very much. I appreciate your testimony, Susan Fisher.

[The prepared statement of Ms. Fisher follows:]

STATEMENT OF SUSAN FISHER, EXECUTIVE DIRECTOR AND EXECUTIVE VICE-CHAIRMAN, DORIS TATE CRIME VICTIMS BUREAU, CARLSBAD, CALIFORNIA

In December of 1987, just a days before Christmas, my 28 year-old brother Ron Ruse was ambushed & shot in the back outside of his apartment in Carlsbad, CA.

Ron was murdered after being stalked for over a year by Linda Ricchio, a woman who had become obsessed with him. Ron had stopped dating Ricchio a few years before the stalking began. He had difficulty extricating himself from the relationship with Ricchio because his attempts to leave would always be followed by her manipulation of him with staged suicide attempts, public scenes meant to embarrass him and threats of violence against him and his friends and family. From the moment that Ron ended their relationship, Ricchio began to access personal information about him in order to track his whereabouts and to know who he talked to and who he spent time with.

She was easily able to get copies of phone bills and utility bills. She was able to trace Ron's fiancée and his fiancée' s mother by accessing DMV information. Since that time, Congress has passed legislation to protect driver's license information. There are loopholes in the current law a that still leave people vulnerable. Senator Feinstein's bill mandates that you must give consent before the information on your diver's license can be sold.

In mid-1987, Ricchio quit her job and stopped going to school in order to pursue Ron on a fulltime basis. She stalked him so relentlessly that she neglected everything else in her life; even letting her cats die of starvation inside her apartment. In November, Ron was compelled to get a restraining order in an attempt to protect himself and save his job. The San Diego County judge who issued the restraining order told him that he should be flattered by the attention. Ricchio's response to the order was to legally purchase a gun and to become proficient in its use, shooting at the head and crotch of a silhouette target.

In late November the daily contacts stopped. We learned later that Linda Ricchio had gone to San Francisco during that period, to visit her brother and to enlist his

help in developing over 200 surveillance photos that she had taken of Ron. During that time Ron moved for the third time in 1987. He was trying to buy a little time, trying to decide what to do, and rapidly coming to the conclusion that there was really nothing that he could do if she decided to become violent. With her ability to track him down, he was convinced that even if he left the state, she would eventually find him using phone records or one of the other kinds of trails that we leave simply by living in the world.

On December 9th, after once again tracing his whereabouts, Ricchio rented the apartment next door to Ron without his knowledge. The two second-story apartments were separated by a privacy wall, Linda's at the back of the balcony and Ron's at the front by the stairs. On Monday, December 14th Ron went home from work in the dark, carrying a bag of groceries, keys and a checkbook. He turned his back to the privacy wall and bent over to put his key in the door. At this point, Ricchio stepped out from behind the wall and shot Ron in the back two times, killing him.

At the time that my brother was killed there were no stalking laws in California. It was not new behavior by any stretch of the imagination; it was simply referred to as harassment or domestic violence. California was the first state to pass a law that specifically made stalking a crime. In the years following my brother's murder, I have been very involved in advocating anti-stalking legislation in California and in working directly with stalking victims; in fact most stalking victims in San Diego County eventually find their way to the Crime Victims Bureau through referrals from law enforcement, DA's and counselors. While many things have changed, both in the criminal justice system and in the way that we view stalkers since my brother's murder in 1987, the pathology of stalking remains the same. We have recently an increased use of internet venues being used, particularly by domestic violence type stalkers to contact and harrass their victims.

And while we have been able to legislate safeguards into many of the avenues of access that stalkers once used to obtain personal information about their victims, new avenues are opening up all the time. Stalkers often have a narcissistic, sociopathithc, borderline personality. This type of person has the intelligence and the drive necessary to access any information available in order to track their victim, and would most certainly be willing to purchase information. Information on the internet that is not safeguarded is fair game.

Everyone should have the ability to protect themselves by protecting personal information about themselves. Senator Feinstein's Privacy Act of 2001 mandates the kind of informed consent necessary to do just that by providing that first, you must be notified if a company intends to sell your personal information, then it provides an avenue for you to stop that sale and it permits you to sue any company that misuses your social security number. This legislation gives individuals increased ability to protect themselves from those who would seek to harm them

Chairperson FEINSTEIN. And now, Doug Comer of Intel. Mr. Comer is the Director of Legal Affairs and Technology Policy for Intel Corporation. He works with the Washington, D.C. Government Affairs Office on issues of legal reform and technology policy. Prior to this time, he served as Deputy and Acting Commissioner of the Patent and Trademark Office for the Department of Commerce. He has also served as Chief Counsel to the Senate Judiciary Subcommittee on Courts, where he was responsible for managing patent, copyright, and trademark legislation during the chairmanship of the Honorable Robert Dole, the former Senator from the State of Kansas.

We welcome you, Mr. Comer.

STATEMENT OF DOUGLAS B. COMER, DIRECTOR OF LEGAL AFFAIRS AND TECHNOLOGY POLICY, INTEL CORPORATION, WASHINGTON, D.C.

Mr. COMER. Thank you, Madam Chairman. I thank you for the opportunity to testify today.

For over three decades, Intel Corporation has been at the forefront of the technology revolution. Intel introduced the world's first microprocessor in 1971 and today we supply the chips, the boards,

the systems, the software, network, and communications equipment that comprise the ingredients of computer architecture and the Internet.

We have heard a lot today about a very important subject, identity theft, and it is precisely because identity theft is closely related to the proper uses of the Internet and of the data that is collected through the Internet that I am here today to express our very strong support for Title I of your bill, which deals with consumer privacy on the Internet.

Our own experience with privacy concerns for consumers really began for us in about 1998 with an experience with a product feature which we introduced in the Pentium III called the processor serial number, which we saw as a simple, effective tool by which a network manager could closely track the performance of computers on a network system. The processor serial number sent an electronic tag along with any communication by the computer in a network identifying the specific machine that that communication was tagged to.

Unfortunately, that feature came to be viewed with great alarm by many in the public sector at large over the possibility that it could be used to assess or facilitate the tracking of the use of computers by the average consumer. We went through a lot of effort to satisfy the concerns of consumers about our desire to protect their privacy and ultimately designed into this processor serial number a feature by which the consumer could turn it off, and ultimately, this was phased out of our products.

But going to your point expressed earlier about the proper balance between privacy and security after the events of 9/11, we were approached by law enforcement authorities who were very interested in the possibility of reviving the processor serial number feature for the very reasons that I have mentioned, because of the ability to tag specific communications to specific computers. We are not going to do that, but the whole experience of the processor serial number drilled a very high awareness at Intel of the importance of respecting consumer privacy for users of the Internet, and out of that experience came a very well-developed program at Intel for managing our own privacy policy, ensuring compliance to fair privacy practices, and working with our vendors and suppliers to do the same.

So identity theft, because of the utility of the Internet, perhaps the most powerful tool for the collection and dissemination ever developed, obviously has fed consumer concerns. The health of the Internet is a core issue for our company and for the entire information technology industry. We believe that these consumer concerns surrounding the safety of online transactions are impeding the growth of e-commerce. We all hear a lot about how the Internet has grown and e-commerce has grown and that is true, but we do not hear about how much more it could grow and be even a more powerful tool of productivity growth in our economy were it not for these concerns.

There is a Gartner survey from about a year ago that shows of 7,000 consumers, 60 percent surveyed said that security and privacy concerns keep them from doing business online. Now, in order to ensure that the Internet continues to grow as a tool of commerce

and a driver for productivity, businesses large and small need to recognize these concerns and respond to them.

So our company has come to the view that Federal privacy legislation is needed not only to address these concerns and to provide a stable playing field for businesses, but also to create an environment where the Internet and the use of the Internet for proper purposes can continue to develop apace.

We think that legislation would clarify the rights for all consumers. It would educate and direct businesses toward the adoption of fair privacy practices. It would create a stable legal structure for businesses to operate in. It would strengthen the U.S. industry position in the ongoing negotiations over the safe harbor agreement with Europe. and it would encourage businesses to migrate into self-regulatory organizations, which are proving to be effective tools for guiding and strengthening businesses in respecting privacy rights of users of the Internet.

It is important, we think, though, that privacy legislation should embrace the following principles which have been subscribed to by all of our major industry associations, such as AEA, ITI, and the Computer Systems Policy Project and others: Mandating notice, ensuring consumer choice, the ability to opt-out of the use of or disclosure of personally identifiable information for purposes unrelated to the transaction for which it is provided, a focus on market solutions—this is where the self-regulatory organizations come in, and providing a national and uniform standard for privacy protection.

A Federal Internet privacy policy should be national in scope and preempt State laws in order to avoid the confusion that would result for users and for website operators by widely disparate local laws. It should, as well, ensure that national standards are not undercut by private litigation case decisions and enforcement, in our view, should be in the Federal courts, subject to FTC supervision. And finally, we think that these principles of legislation should apply to offline data collection, as well.

In Intel—

Chairperson FEINSTEIN. Would you repeat that last sentence?

Mr. COMER. These principles should apply to offline data collection, as well. In our view, this can be done efficiently if data collection materials such as warranty cards and the like are designed properly. All of this data is ultimately reduced to electronic form and there is really no reason for differentiation between online collection and offline collection.

So taking all of these principles into consideration, we at Intel commend you, Senator Feinstein, for you focus on the need for a comprehensive, systematic, national approach to protecting privacy and we strongly support the provisions of Title I of your bill addressing consumer privacy on the Internet because it reflects these principles.

Because we share your objective of comprehensive protection for the Internet user, we believe that the rules set forth in S. 1055 should also apply to public sector websites, as well. We have seen cases where data collected from the public by government agencies has been transferred without the consent of the parties supplying the data to private sector entities for commercial purposes. Again,

a consumer should be protected no matter what websites or type of websites they are going to.

I would like to take this opportunity to submit for the subcommittee's consideration a letter signed by Mr. Bill Archey, President of the American Electronic Association, in support of Title I of your bill and I provided that to your staff and to the committee, and also ask for inclusion in the record of a statement of Mr. Jeff Nicol, our Privacy Program Manager, which was prepared for the original scheduling of this hearing back last fall.

Chairperson FEINSTEIN. They will be added to the record.

Mr. COMER. Thank you.

In sum, we believe that the continuing viability of the Internet marketplace depends upon good rules, good practices, and good policing. Congress should lay down the rules, depend upon the self-regulatory tools now in the marketplace to advance the adoption of fair privacy practices, and give responsibility for the enforcement of these rules to the FTC and the State attorneys general. In this way, we think that bad actors will, over time, be driven out of the marketplace and consumer acceptance of the Internet as a safe place to do business will be secured. The Internet will then flourish as one of the most efficient, if not the most efficient, market tools ever developed.

That concludes my remarks and I will be pleased to answer questions.

Chairperson FEINSTEIN. Thanks very much, Mr. Comer.

[The prepared statement of Mr. Comer follows:]

STATEMENT OF DOUGLAS B. COMER, DIRECTOR, LEGAL AFFAIRS AND TECHNOLOGY POLICY, INTEL CORPORATION

I thank the Chair for the opportunity to testify this afternoon. My name is Doug Comer and I am Director of Legal Affairs and technology policy for Intel Corporation. For over three decades, Intel Corporation has been at the forefront of the technology revolution. Intel introduced the world's first microprocessor in 1971. Today, Intel supplies chips, boards, systems, software, networking and communications equipment that comprise the "ingredients" of computer architecture and the Internet. The health of the Internet is a core issue for our company and for the entire Information Technology industry.

Intel believes that consumer concerns surrounding the safety of online transactions are impeding the growth of e-commerce. For example, a Gartner survey of 7,000 consumers found that 60% say that security and privacy concerns keep them from doing business online.[1] In order to ensure that the Internet continues to grow as a tool of commerce and a driver for productivity in our economy, businesses large and small need to recognize these concerns and respond to them.

Our company has come to the view that federal privacy legislation is needed to address these concerns, and provide a stable legal playing field for business. We believe that such legislation should embrace the following principles, which have been subscribed to by all of our major industry associations:

Mandate notice—Websites that collect personally identifiable information should provide clear and conspicuous notice of their practices at the time of information collection.

Ensure consumer choice—Internet users should have the ability to opt-out of the use or disclosure of their personally identifiable information for purposes unrelated to the transaction for which it is provided.

Focus on market solutions—Legislation should build upon existing self-regulatory mechanisms, and back those mechanisms with the enforcement clout of the Federal Trade Commission.

---

[1] Jeff Sweat, "Privacy—Can Businesses Build Trust and Exploit Opportunity?—As the opportunities to use personal data for marketing grow, companies search for how to strike the right balance between delivering the service customers want and the privacy they expect," *Information Week* (August 20, 2001) 30.

Provide a national, uniform standard for privacy protection—A federal Internet privacy policy should be national in scope, and preempt state laws in order to avoid the confusion that would result for users and for website operators by widely disparate local laws. It should, as well, ensure that the national standards are not undercut by private litigation case decisions. The enforcement should be in federal court, subject to FTC supervision.

Apply the same principles to Offline data collection—The same privacy principles should apply regardless of whether the transaction was conducted online or offline. In Intel's view, this can be done efficiently if data collection materials—such as warranty cards, etc.—are designed properly.

We at Intel commend you, Senator Feinstein, for your focus on the need for a comprehensive, systematic, and national approach to protecting privacy. We strongly support the provisions of Title I of your bill, which addresses consumer privacy on the Internet, because it reflects these principles.

Because we share your objective of comprehensive protection for the Internet user, we believe that the rules set forth in S. 1055 should apply to public sector websites as well. We have seen cases where data collected from the public by government agencies has been transferred, without the consent of the parties supplying the data, to private sector entities for commercial purposes.

I would take this opportunity to submit for the Subcommittee's consideration a letter signed by Mr. Bill Archey, President and CEO of the American Electronics Association, that expresses the positive views of that very important organization on the provisions of Title I of your bill. I also ask for inclusion in the record of the testimony of Mr. Jeff Nicol, Customer Privacy Manager at Intel, which was previously provided to the Committee and which I have appended to my statement.

That concludes my remarks. I will be glad to answer any questions the members of the Subcommittee may have.

Chairperson FEINSTEIN. I would like to introduce John Avila. Mr. Avila serves as the Executive Counsel for Walt Disney Company in Burbank, California. His responsibilities include data privacy law counseling for the domestic and international operations of Disney's offline and online businesses. Prior to his time at Disney, Mr. Avila served as Chief Privacy Officer of a venture capital-funded Internet company and as litigation counsel to CBS Broadcasting. Mr. Avila has spoken publicly numerous times on the subjects of data privacy and First Amendment rights.

Mr. Avila, welcome.

STATEMENT OF JONATHAN D. AVILA, EXECUTIVE COUNSEL, WALT DISNEY COMPANY, BURBANK, CALIFORNIA

Mr. AVILA. Thank you very much, Senator. I am pleased to appear here today on behalf of the Walt Disney Company to testify in support of S. 1055, the Privacy Act of 2001. Protecting the privacy and security of personally identifiable information is a critical national and international concern and a matter of high priority at Disney. As one of the most trusted names in American business, it is vital to us at Disney that our guests and customers know that we are concerned about the privacy of the information they give us and that we will treat their information appropriately.

As a result, we are developing our own statement of privacy principles, which are largely similar to those set forth in the Privacy Act of 2001 and which will apply to both our online and offline activities. Because our primary business is not health care or finance, my comments today, however, are restricted to the matters addressed in Title I of the proposed statute and our suggestion that a provision relating to the security of consumer data be added to Title I of the statute.

With respect to the matter of notice, we support the principle found in Section 101(b) that adequate notice requires a disclosure

of the type of information being sought, the purpose for which the information will be used, and with whom, if anyone, the information may be shared. We agree, of course, that to be meaningful, any notice must be clear and understandable to the consumer and must be given prior to any marketing use or sharing of the consumer's data.

With respect to the matter of choice, a substantial argument can be made that consumers should affirmatively give permission for any use of personally identifiable information, that is a so-called opt-in consent.

Nonetheless, we believe the bill draws a reasonable distinction between general information and matters such as Social Security numbers and information held by financial institutions and health care providers. These latter types of information are so sensitive that appropriate protection of personal privacy requires that the individual providing the information affirmatively express a willingness to have the information disclosed to others.

Although there may well be other categories of information that also deserve this special type of protection, the same degree of sensitivity is generally not present in the information sought in a typical commercial transaction and, hence, an opt-out provision may be sufficient.

Because we believe our guests should have the right to opt-out of receiving marketing materials from Disney, as well as having us not share their information with third parties, our privacy principles will provide multiple choices for our guests. Thus, a guest may elect to receive marketing or other information from Disney but opt-out of our sharing of any of the guest data with third parties. Or the guest may simply opt not to receive any marketing information at all from Disney and our related companies.

In this regard, let me now voice some concern about the scope of Section 101(a) of the Act. There, the Act proposes to limit its coverage to, one, disclosure of personally identifiable information to non-affiliated third parties for marketing purposes, and two, sale of such information to non-affiliated third parties.

In keeping with our view of consumer privacy, we believe this subsection should be modified to extend the Act's purview to all commercial sharing of personally identifiable information with non-affiliated third parties. In turn, the exception provided by Subsection (a)(2) should be broadened to track in appropriately modified form the exceptions provided by Section 502 of the Gramm-Leach-Bliley Act.

In this manner, consumers would be protected against all improper and unauthorized disclosure of their personal information to non-affiliated third parties. At the same time, non-financial businesses would have the same flexibility that financial institutions enjoy to disclose information for legitimate purposes, such as to prevent fraudulent transactions, comply with governmental regulatory requirements, and outsource marketing and fulfillment functions to entities that are contractually obligated to respect the confidentiality of their customers' data.

Turning to the matter of security, we at Disney believe that the privacy of personal information is only as strong as the security measures that protect that information. We therefore suggest add-

ing to the bill a requirement that entities that collect consumers' personal information maintain reasonable security measures to safeguard the confidentiality of that information. Of course, for general consumer information, such as that covered by Title I of this legislation, those security measures need not be as elaborate as the measures that apply to the sensitive data held by financial institutions and health care providers.

Perhaps the most important provision of this measure is Section 105, which provides for preemption of State, common, and statutory law. Broad Federal preemption is critical to this or any similar legislation. As we all know, the Internet has shrunken our world further than we could ever have imagined. As a result, information given in one jurisdiction can appear in another in a nanosecond.

While the international implications of this fact are themselves daunting, the prospect of the several States acting to address these issues in varying and perhaps conflicting ways is horrifying. One of the great strengths of our country lies in the integration of our national economy under Federal control over interstate commerce. Without broad Federal preemption in this area, the inevitable patchwork of State laws will present a formidable barrier to commerce and will, in essence, cede what should be a Federal mandate to the parochial interests of the various States.

American business simply cannot operate efficiently under a myriad of conflicting rules governing national economic activity. Thus, it is vital that, at least for the United States, there be a single set of rules on this subject mandated through Federal legislation and preemption.

In closing, we at the Walt Disney Company congratulate you, Senator Feinstein, on the bill's approach to balancing the need for governmental regulation with responsible action through FTC-approved safe harbor programs. Indeed, as I mentioned at the outset, we soon will be backing our commitment to our guest privacy with the adoption of our own voluntary privacy principles.

Thank you. I would be pleased to answer any questions the subcommittee may have.

Chairperson FEINSTEIN. We will have some, and thank you very much.

[The prepared statement of Mr. Avila follows:]

STATEMENT OF JONATHAN D. AVILA, EXECUTIVE COUNSEL, THE WALT DISNEY COMPANY

Good afternoon. My name is Jonathan Avila and I am pleased to appear here today on behalf of The Walt Disney Company to testify in support of Senate Bill 1055, the "Privacy Act of 2001."

Protecting the privacy and security of personally identifiable information is a critical national and international concern, and a matter of high priority at Disney. As one of the most trusted names in American business, it is vital to us at Disney that our guests and customers know that we are concerned about the privacy of the information they give us and that we will treat their information appropriately.

As a result, we are developing our own Statement of Privacy Principles, which are largely similar to those set forth in the Privacy Act of 2001 and which will apply to both our online and offline activities. Because our primary business is not healthcare or finance, my comments today, however, are restricted to the matters addressed in Title I of the proposed statute, and our suggestion that a provision relating to the security of consumer data be added to Title I of the statute.

NOTICE

With respect to the matter of notice, we support the principle found in Section 101(b) that adequate notice requires a disclosure of the type of information being sought, the purposes for which the information will be used and with whom, if anyone, the information may be shared. We agree, of course, that, to be meaningful, any notice must be clear and understandable to the consumer, and must be given prior to any marketing use or sharing of the consumer' s data.

CHOICE

With respect to the matter of choice, a substantial argument can be made that consumers should affirmatively give permission for any use of personally identifiable information (that is, a so-called "opt-in" consent). Nonetheless, we believe the Bill draws a reasonable distinction between general information, and matters such as social security numbers and information held by financial institutions and health care providers. These latter types of information are so sensitive that appropriate protection of personal privacy requires that the individual providing the information affirmatively express a willingness to have the information disclosed to others.

Although there may well be other categories of information that also deserve this special type of protection, the same degree of sensitivity is generally not present in the information sought in a typical commercial transaction and hence an opt-out provision may be sufficient.

Because we believe our guests should have the right to opt out of receiving marketing materials from Disney, as well as having us not share their information with third parties, our Privacy Principles will provide multiple choices for our guests. Thus, a guest may elect to receive marketing or other information from Disney, but opt out of our sharing any of the guest's data with third parties. Or, the guest may simply opt not to receive any marketing information at all from Disney and our related companies.

In this regard, let me now voice some concern about the scope of Section 101 (a) of the Act. There, the Act proposes to limit its coverage to: (1) disclosure of personally identifiable information to nonaffiliated third parties for marketing purposes; and, (2) sale of such information to nonaffiliated third parties. In keeping with our view of consumer privacy, we believe this subsection should be modified to extend the Act's purview to all commercial sharing of personally identifiable information with nonaffiliated third parties. In turn, the exception provided by Subsection (a) (2) should be broadened to track, in appropriately modified form, the exceptions provided by Section 502 of the Gramm-Leach-Bliley Act. In this manner, consumers would be protected against all improper and unauthorized disclosure of their personal information to nonaffiliated third parties. At the same time, non-financial businesses would have the same flexibility that financial institutions enjoy to disclose information for legitimate purposes, such as to prevent fraudulent transactions, comply with governmental regulatory requirements, and outsource marketing and fulfillment functions to entities that are contractually obligated to respect the confidentiality of their customers' data.

SECURITY

Turning to the matter of security, we at Disney believe that the privacy of personal information is only as strong as the security measures that protect that information. We therefore suggest adding to the Bill a requirement that entities that collect consumers' personal information maintain reasonable security measures to safeguard the confidentiality of that information. Of course, for general consumer information, such as that covered by Title I of this legislation, those security measures need not be as elaborate as the measures that apply to the sensitive data held by financial institutions and health care providers.

PREEMPTION

Perhaps the most important provision of this measure is Section 105, which provides for preemption of state common and statutory law. Broad federal preemption is critical to this or any similar legislation. As we all know, the Internet has shrunken our world further than we could ever have imagined. As a result, information given in one jurisdiction can appear in another in a nanosecond. While the international implications of this fact are themselves daunting, the prospect of the several States acting to address these issues in varying and perhaps conflicting ways is horrifying.

One of the great strengths of our country lies in the integration of our national economy under federal control over interstate commerce. Without broad federal preemption in this area, the inevitable patchwork of state laws will present a formidable barrier to commerce and will, in essence, cede what should be a federal mandate to the parochial interests of the various States. American business simply cannot operate efficiently under a myriad of conflicting rules governing national economic activity. Thus, it is vital that, at least for the United States, there be a single set of rules on this subject mandated through federal legislation and preemption.

In closing, we at The Walt Disney Company congratulate Senator Feinstein on the Bill's approach to balancing the need for governmental regulation with responsible private action through FTC-approved Safe Harbor programs. Indeed, as I mentioned at the outset, we soon will be backing our commitment to our guests' privacy with the adoption of our own voluntary Privacy Principles.

Thank you. I would be pleased to answer any questions the sub-committee may have.

Chairperson FEINSTEIN. Senator Kyl, I understand there is going to be a vote at 4:20. My suggestion is that we go and hear Mr. Torres and then we can decide whether we spell each other or take a recess.

Mr. Torres is the Legislative Counsel in Washington for the Consumers Union. He is responsible for advocating for consumers before Congressional agencies and the Federal Reserve Board on issues related to financial services. Mr. Torres's area of expertise includes privacy, electronic commerce, and consumer credit.

We welcome you, Mr. Torres.

STATEMENT OF FRANK TORRES, LEGISLATIVE COUNSEL, CONSUMERS UNION, WASHINGTON, D.C.

Mr. TORRES. Thank you, Madam Chairwoman and Senator Kyl. It is a pleasure to be here and we appreciate the opportunity to testify before the committee today and are grateful that you have once again turned your attention to the serious topic of consumer privacy.

Before I get into my testimony in earnest, though, I wanted to respond to an earlier question about where consumers can go, where can victims of identity theft go for help. In addition to Consumer Reports magazine, which has written through the years on the topic of identity theft and how consumers can protect their privacy, Beth Givens at the Privacy Rights Clearinghouse is a tremendous source of information for victims of identity theft and how consumers can prevent it. Her website is at www.privacyrights.org and she actually has a fact sheet, "Identity Theft: What To Do If It Happens To You," that goes step by step of all the different areas, all the different places that you should think about contacting if you are the victim of identity theft, from the credit bureaus on down.

In addition, I believe that the FTC's website has a new feature and that is an affidavit, a model affidavit that consumers can use to submit to the different credit bureaus and creditors if they are victims of identity theft.

S. 1055 will protect security numbers, prevent identity theft, and maybe put an end to some of the tragic stories we have heard here today. Given the severity of identity theft and its cost to both business and consumers, it is crucial that the selling and sharing of Social Security numbers be curbed. I would like to focus my testimony today, however, on some of the other privacy aspects of this bill. How times have changed when we have got forward-thinking

companies advocating Federal privacy laws, and we have two of them here today and we appreciate their efforts on moving the debate on privacy forward.

Consumers Union has advocated in favor of strong privacy protections. With other consumer and privacy advocates, we have pushed for privacy amendments to the Gramm-Leach-Bliley Act. We fought for strong medical privacy regulations and are part of a broad coalition that supports online privacy protections. Here are some of the reasons we believe this bill is good.

First, the comprehensive approach of S. 1055 will provide both consumers and businesses with clear expectations of how information will be treated, when it can be shared, and how the flow of information can be controlled. Those protections will be in place wherever information is gathered. Whether privacy is lost because a website places a cookie on a personal computer or because information is obtained from a warranty card does not really make a difference to the consumer. Both are troubling invasions of privacy.

Applying privacy protections in both online and offline settings is a fresh approach. Up to now, privacy has been addressed sector by sector. Often, we hear complaints from businesses that one sector is being treated differently from another. S. 1055 responds to those concerns.

Second, S. 1055 advances the privacy debate by recognizing the distinction between sensitive and non-sensitive data. We have commented that more sensitive personal data, like financial and medical information, warrant the strongest possible protections. A business should first obtain a consumer's consent before collecting or sharing that information. Where data is used solely for marketing purposes, a less rigorous approach may be enough. We encourage providing specific, uniform, and up-front mechanisms for exercising this opt-out, especially after seeing what happened with the notices required under the Gramm-Leach-Bliley Act. We also support the bill's prohibition on denying service to consumers refusing to grant consent to data sharing.

Third, S. 1055 offers a substantial improvement over the privacy provisions of the Gramm-Leach-Bliley Act by providing that financial information cannot be shared with third parties without express consent of consumers. This discussion about privacy should also consider other areas.

Consumers Union believes that it is critical to seek input from the States before deciding to preempt State privacy efforts. We would not support legislation preempting State laws where the Federal law is weak. States like California are moving forward with strong privacy bills similar to some of the provisions in S. 1055. While Congressional efforts may lag these State initiatives, sponsors of those bills should take note that they are on target with Federal proposals.

It should also be clear that S. 1055 will not roll back existing laws, such as the consumer privacy protections in the Communications Act. Just yesterday, Comcast, one of the largest cable TV providers in the country, abandoned collecting data from their subscribers. This collecting was done in violation of the law in which Congress placed a high priority on protecting customer viewing habits.

We also support other efforts to curb identity theft and assist victims, like the Reclaim Your Identity Act recently introduced by Senator Cantwell.

Last but not least, the selling and sharing of Social Security numbers between businesses warrants scrutiny. In some cases, it may open the door to abuses.

In summary, S. 1055 does not ban the collection and use of personal data. It merely gives consumers control over their own information and it places a burden on businesses that want information to convince consumers to share it. That sounds like how the marketplace should be working.

Thank you, and I would be happy to answer any questions.

Chairperson FEINSTEIN. Thank you very much, Mr. Torres.

[The prepared statement of Mr. Torres follows:]

STATEMENT OF FRANK TORRES, LEGISLATIVE COUNSEL FOR CONSUMERS UNION

Consumers Union[1] appreciates the opportunity to present this testimony on the *Privacy Act of 2001, S. 1055*. This hearing provides a forum to discuss why American consumers need meaningful and comprehensive privacy protections.

Consumers Union has long been an advocate for strong privacy protections. Along with other consumer and privacy advocates we pushed for amendments to the Gramm-Leach-Bliley Act to try to provide consumers control over how their personal financial information is collected and whether it could be shared. We fought for strong medical privacy regulations and continue to push for privacy related to health like genetic information. Consumers Union is also part of a broad privacy coalition that has supported online privacy protections.

Stronger laws are needed to give consumers control over the collection and use of their personal information. Legislative efforts, such as S. 1055 will help ensure that consumers are told about how and why information is collected and used, provided access to that data, and given the ability to choose who gets access to their most intimate personal data.

There are a number of elements of privacy protection that have become clearer over the course of our involvement in the privacy debate which are reflected in S. 1055:

• A comprehensive approach to privacy protection, like S. 1055, is warranted. For consumers, the comprehensive approach of S. 1055 has advantages clear expectations of how their information will be treated, when it can be shared and how the flow of information can be controlled. The distinctions between privacy intrusions are sometimes lost on consumers. Whether privacy is lost because of a cookie placed on a personal computer after visiting a website or because information obtained from a warranty card is collected and sold it really does not make a difference. Applying privacy protections in both online and offline settings is a fresh approach that has merit considering how the privacy debate has developed. Up to now the approach to privacy has been sector by sector. There are bills on financial privacy, medical privacy and online privacy. Often we hear complaints that one sector is being treated differently than another. S. 1055's comprehensive approach addresses those concerns. If industry wants fair and clear rules that treats everyone the same, they should be supportive of S. 1055's comprehensive approach.

• A distinction can be made between sensitive and non-sensitive information. S. 1055 advances the privacy debate by recognizing the distinction between sensitive and non-sensitive data. We have commented that more sensitive personal data, like financial and medical information, warrant the strongest possible protections. For

[1] Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health, and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of Consumer Reports, its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, Consumer Reports with approximately 4.5 million paid circulation, regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

this type of data we favor an approach that requires a business to obtain the consumer's consent prior to sharing that data.

Provided other data collected is used solely for marketing purposes a lessor standard may be appropriate. We support this approach only if clear notice is given to the consumer prior to the collection of the data and that the consumer is given the opportunity up front to choose not to have his or her information shared with others. We encourage providing specific and uniform mechanisms for exercising an opt-out. Several states are implementing "do-not-call" lists. Even the Direct Marketing Association maintains such a list. A one-stop universal opt-out would be a useful tool for consumers. The Federal Trade Commission has recently published a proposed rule for a national do-not-call list.

• Consumers need a stronger law to protect their personal financial information. S. 1055 offers a substantial improvement over the privacy provision of the Gramm-Leach-Bliley Act by providing that financial information cannot be shared with third parties without the express consent of the consumers. The Gramm-Leach-Bliley Act falls far short of providing meaningful privacy protections in the financial setting. Loopholes in the law and in this draft rule allow personal financial information to be shared among affiliated companies without the consumer's consent. In many instances, personal information can also be shared between financial institutions and unaffiliated third parties, including marketers, without the consumers consent. Consumers across the country are receiving privacy notices from their financial institutions. Unfortunately these opt outs, in reality, will do little or nothing to prevent the sharing of personal information with others. Other loopholes allow institutions to avoid having to disclose all of their information sharing practices to consumers. In addition, the GLB does not allow consumers to access to the information about them that an institution collects. While states were given the ability to enact stronger protections, those efforts have met fierce resistance by the financial services industry.

• Consumers' health information should not be shared without their express consent. S. 1055 protects personal health information across the board under the bill health information cannot be shared without the prior consent of the consumer.

• The sale of social security numbers to the public should be banned. Public disclosure of social security numbers should be limited. Businesses should be prohibited from denying services if a consumer does not wish to provide a social security number in certain circumstances. S. 1055 shuts down many avenues that lead to the release of social security numbers.

• Commercial entities that collect personal information should be responsible for providing notice to consumers if they intend to share personal data with others and allow consumers to opt-out of such data collection and sharing third parties. S. 1055 requires notice and consent prior to the sharing of personal information with a non-affiliated entity.

Sound and comprehensive privacy laws will help increase consumer trust and confidence in the marketplace and also serve to level the playing field. These laws do not have to ban the collection and use of personal data, merely give the consumer control over their own information.

The remainder of these comments provide greater detail on privacy issues related to marketing, financial data, health data, and identity theft.

MARKETING

Consumers face aggressive intrusions on their private lives. Often a consumer is forced to provide personal information to obtain products or services. Many times information that has been provided for one purpose is then used for another reason, unbeknownst to the consumer. Financial institutions, Internet companies health providers and marketers have been caught crossing that line. Meanwhile, identity theft is at an all time high.

Increasingly, consumers want to choose who does and does not have access to their medical, financial and other personal information.[2] If access is needed consumers want to be able to specify for what purposes and to what extent access will be granted. Consumers want assurances that the information they consider sensitive will be kept private by the businesses they use. Often, consumers have no

[2] Consumers continue to care about their privacy. A recent survey by Forester Research found that 72% of consumers participating in the study said that it was an extreme violation of their privacy for businesses to collect and then supply data about them to other companies. Another survey by Public Opinion Strategies found that strengthening privacy laws to assure that medical, financial, or personal records are kept private is one of the highest-rated issues of concern to consumers nationwide.

choice in whether or not information is collected and no choice in how it is used. Today, any information provided by a consumer for one reason, such as getting a loan at a bank, can be used for any other purposes with virtually no restrictions.

• S. 1055 will allow consumers to opt-out of sharing of information with third parties for marketing purposes. This requirement should be easy to implement, in most cases consumer choice can be provided at the point where the information is collected. Consumers are sometimes given that choice today in both online and offline settings.

• The opt-out for marketing purposes is distinguishable from a stricter regime for the collection and use of sensitive financial and health information. So long as the information collected is used solely for marketing purposes, an opt-out approach may be adequate provided notice and choice is provided up front, prior to the collection of the data, and that the notice and choice is clear and in plain English. The opt-out must be easy for consumers, unlike the opt-out under the Gramm-Leach Bliley Act. The opt-out provided by most financial institutions have proven difficult for consumers to understand and hard to exercise.

If properly provided the notice and opt-out contemplated in this legislation could result into a system where consumers may indicate that they want no calls, then individually choose, on a case-by-case, merchant -by-merchant basis, to consent to information collection and use by parties they trust or believe will provide some benefit.

• Exceptions to the opt-out requirement should be minimal. The exceptions provided in the legislation appear to be reasonable and should not be expanded.

• It is appropriate to allow the Federal Trade Commission to have enforcement authority. The FTC has taken a leadership role in protecting consumer privacy. The agency was given specific authority under the GLB to implement those privacy provisions. In addition it has held numerous workshops and convened advisory committees on the issue of privacy.

• The use of seal programs to provide for a safe harbor needs strict scrutiny and oversight. Consumers Union, and many other advocacy organizations remain skeptical of the ability of industry groups to self-regulate. Seal programs are often dependent on the very firms they are supposed to scrutinize. If a safe harbor remains in the bill, there should also be a mechanism to evaluate whether the program is effective and ensure that the requirements of the program are as strict as the protections contained in the bill.

• Consumers Union believes that it is critical to seek the input from the states, including state attorneys general and legislators, before deciding to preempt state privacy efforts.

FINANCIAL PRIVACY

Consumers have reason to be concerned about how their private financial information is being collected, used, shared and sold. Under the GLB there are no limits on the ability of a financial institution to share information about consumers' transactions, including account balances, who they write checks to, where they use a credit card and what they purchase, within a financial conglomerate. Because of loopholes in GLB, in most cases sharing a consumer's sensitive information with a third party is allowed too. All the exceptions created by GLB make it difficult to come up with a list of circumstances where personal financial information cannot be shared.

Financial institutions promised that in exchange for a virtually unfettered ability to collect and share consumers' personal information, that consumers would get better quality products and services and lower prices. This is why, they claimed, consumers shouldn't have strong privacy protections like the ability to stop the sharing of their information among affiliates, or access to that information to make sure its accurate.

Bank fees for many consumers continue to rise. Information about financial health may actually be used to the consumer's determent if it is perceived that the consumer will not be as profitable as other customers. Both Freddie Mac and Fannie Mae say between 30 and 50% of consumers who get subprime loans, actually qualify for more conventional products, despite all the information that is available to lenders today. Credit card issuers continue to issue credit cards to imposters, thus perpetuating identity theft, even when it seems like a simple verification of the victim's last known address should be a warning. Instead of offering affordable loans, banks are partnering with payday lenders. And when do some lenders choose not to share information? When sharing that information will benefit the consumer—like good credit histories that would likely mean less costly loans.

Chase Manhattan Bank, one of the largest financial institutions in the United States, settled charges brought by the New York attorney general for sharing sensitive financial information with out-side marketers in violation of its own privacy policy. In Minnesota, U.S. Bancorp ended its sales of information about its customers' checking and credit card information to outside marketing firms. Both of these were of questionable benefit for the bank's customers. Other institutions sold data to felons or got caught charging consumers for products that were never ordered.

Consumers should have the right to be fully and meaningfully informed about an institution's practices. Consumers should be able to choose to say "no" to the sharing or use of their information for purposes other than for what the information was originally provided. Consumers should have access to the information collected about them and be given a reasonable opportunity to correct it if it is wrong. In addition to full notice, access, and control, a strong enforcement provision is needed to ensure that privacy protections are provided.

• S. 1055 requires that consumers opt-in before financial information can be shared with third parties.

• S. 1055 also provides that a consumer cannot be denied service for refusing to consent to the sharing of his or her information.

• The exceptions contained in S. 1055 are limited to reasonable expectations related to the primary use of personal data.

• Legislative efforts in this body, like S. 1055, send a strong message to those in the states pursuing similar privacy protections. It is clear that states, like California, are on the right tract in pushing forward with bills like California Senate Bill 773, which will provide strong financial privacy protections in that state. While congressional efforts may lag these state initiatives, sponsors of those bills should take note that they are on target with what federal legislators are considering.

MEDICAL PRIVACY

Medical information has been used for inappropriate purposes. The medial privacy rule promulgated by the Department of Health and Human Services highlighted a number of cases where private medical information was released for profit and marketing purposes completely unrelated to the treatment of those patients. A USA Today editorial earlier this year highlighted the consequences of a failure to protect medical privacy. The editorial cited various privacy intrusions an employer firing an employee when they got the results of a genetic test; release of medical records to attack political opponents; and hackers getting access to health records from a major University medical center (USA Today, March 20, 2001).

Patients should not be put in the position of withholding information or even lying about their medical conditions to preserve their privacy. Those seeking medical treatment are most vulnerable and should be allowed to focus on their treatment or the treatment of their loved ones, rather than on trying to maintain their privacy. It is unfair that those citizens must be concerned that information about their medical condition could be provided to others who have no legitimate need to see that information.

• S. 1055 requires a customer's affirmative consent before individually identifiable health information can be shared across the board. The bill extends the protections of the HHS rules to cover any setting across the board.

IDENTITY THEFT

Beth Givens of the Privacy Rights Clearinghouse estimates that there were 500,000 to 700,000 victims of identity theft last year. The number of complaints to the FTC almost doubled from March to December 2001. It is very easy to obtain social security numbers. Non-social security administration uses of social security numbers have not been prohibited. As a result, social security numbers are used as identification and account numbers by many entities.

The Internet provides an easy and cheap way to get personal information. Web sites sell individuals' social security numbers, some for as little as $20. Self-regulatory efforts by information brokers has been in effective in restriction the sale of sensitive personal information to the general public.

Other elements to consider are the practices of the credit and credit reporting industries. They must also work to prevent fraud and help victims recover from identity theft. Many consumers have no idea how they become victims of identify theft. Often, they do not find out their personal information has been misused for more than a year, and sometimes as long as five years. Victims must spend significant amounts of time contacting creditors and credit reporting agencies in order to repair

the damage done to their credit histories. In the meantime, they are often unable to obtain credit and financial services, telecommunication and utility services, and sometimes employment.

The expanded use of the SSN as a national identifier has given rise to individuals using counterfeit SSNs and SSNs belonging to others for illegal purposes. Stolen SSNs have been used to gain employment, establish credit, obtain benefits and services, and hide identity to commit crimes.

One of the unfortunate results of the events of last September are reports of identity theft scams. Criminals have tried to obtain data from the unsuspecting families of victims of that tragedy. This should remind creditors that they have a responsibility to verify the identity of individuals prior to issuing lines of credit.

The FTC is taking steps to assist the victims of identity theft, but it is also important to focus on preventing the theft in the first place. As an FTC official recently stated, " in this day of remote transactions and greater access to publicly available information on each of us, identity theft has never been easier to commit."

• S. 1055 helps take Social Security numbers out of circulation. It would prohibit the commercial sale of SSNs. The bill would also limit uses of SSN s by private sector entities and stop the display of SSNs by government agencies.

• S. 1055 provides civil penalties for misuse of SSNs. We believe a private right of action provides consumers with a meaningful safeguard against businesses who should be held accountable for the misuse of SSNs.

• The legislation is a useful step in protecting SSNs and curbing identity theft. Given the severity of identity theft, and the cost to both business and consumers, there remains a need to monitor and assess the effectiveness of any legislation designed to prevent this problem.

Chairperson FEINSTEIN. I just want to enter into the record that I am very pleased to also add to the support of this bill eBay, NCR, the American Medical Association and Pacific Life Insurance Company. I want to indicate that this bill did not just emerge. It has been worked on over a substantial period of time and I wanted to thank everybody at the table who has helped us with this. It is a new area. I think it does provide the national floor, so to speak. It preempts State law in that sense. It does apply to online/offline.

I would like to begin my questions, if I can, with a question of Mr. Avila because I did not quite understand. I am reading Section 101 of my bill and also Section 502 of Gramm-Leach-Bliley and I did not understand the point that you were making.

Mr. AVILA. We are concerned, Senator, that we believe that privacy protection should be extended to all sharing, commercial sharing of information with third parties, but if that is done, then the exception in S. 1055 needs to be broadened somewhat because it covers—it is now specific to the limitations on sharing that are in the bill.

Chairperson FEINSTEIN. How would you broaden it? What would you add to it?

Mr. AVILA. We would suggest not restricting the coverage to sale of personal information to non-affiliated third parties and leave the statute disclosure for marketing purposes. We believe it should apply to any purpose for which personal information is disclosed to a third party.

Chairperson FEINSTEIN. That was the point you were making, Mr. Comer, is that right?

Mr. COMER. My point was slightly different, which was I was suggesting that the bill should apply, as well, to public websites. Perhaps that is what you were thinking of when I was talking about that there should not be—

Chairperson FEINSTEIN. Right. Do you agree with the point Mr. Avila is making?

Mr. COMER. I agree in the sense that we think that the restrictions on disclosure or use or sale should all be embraced or encompassed within the privacy protections that you articulate. We can work with your staff on this if there is a perceived gap.

Chairperson FEINSTEIN. All right. We appreciate that.

Mr. TORRES. Senator?

Chairperson FEINSTEIN. Mr. Torres?

Mr. TORRES. If I might, I have got some concerns about extending the—including any more exceptions when we are talking solely about the use of this information for marketing purposes. Section 303 of S. 1055 does incorporate for purposes of the sale of financial information and the use of financial information the Section 502 exclusions under Gramm-Leach-Bliley and some of those are reasonable in the context of servicing accounts and making sure that the consumer is able to correspond and those types of things.

So we would be happy to work with your staff as to whether or not any of those types of exceptions might be reasonable, but at this point, we would be skeptical about opening it up for marketing, when you are talking about using information for marketing purposes.

Chairperson FEINSTEIN. Mr. Avila, I tend to come down on Mr. Torres's side on that and I do not understand why you would want this.

Mr. AVILA. We simply believe that sharing should—that the coverage of the statute should not be restricted to sharing with third parties for marketing purposes but it should cover any purpose for which information is shared.

Chairperson FEINSTEIN. Like what?

Mr. AVILA. Well, there may be other purposes that are not specifically for marketing, but any commercial purpose. Marketing seems to be, to us, too limited.

Chairperson FEINSTEIN. You do not think that is the barn door through which the Mack truck can be driven?

Mr. AVILA. Well, Senator, we are proposing extending not the exceptions but the coverage of the statute.

Chairperson FEINSTEIN. Oh, I see. All right.

Mr. AVILA. And then, as a consequence of that—

Chairperson FEINSTEIN. I misunderstood, then. I thought you were—

Mr. AVILA. Yes.

Chairperson FEINSTEIN. Then I think we are all on the same wavelength—

Mr. AVILA. Now, naturally—

Chairperson FEINSTEIN [continuing]. So we ought to be able to work that out.

Mr. AVILA. Naturally, if the coverage were extended, the exceptions would have to conform to the extension of the coverage, so, for example, fraud prevention and other reasonable exceptions should follow the extension of the purview of the covered portions of the Act.

Chairperson FEINSTEIN. Right. I think that is excellent. I think we can work it out. Perhaps while you are all here, you can sit down with the staff and do some wordsmithing.

I gather the safe harbor provisions that exempts businesses with good privacy protections from government regulation, it is my understanding that Disney is a member of the TRUSTe Privacy Program, a seal program that sets minimum privacy standards. I want to ask you, what are your views of the safe harbor provisions of this bill? I want to ask also this question. Does Disney regularly review its data collection operations to ensure compliance with its own privacy standards?

Mr. AVILA. As to your first question, Senator, we are members of the TRUSTe seal program. We believe that TRUSTe has made important strides in formulating a structure for protecting consumers' online privacy. The gap in the protection online is not for seal participants but rather for non-seal participants, and since the TRUSTe program and the BBB Online program are not compulsory, they do not cover the actions of the so-called bad actors who choose not to participate in those programs and who do not follow the regime of protection that those programs mandate.

We believe that the safe harbor provisions of the Act are a highly appropriate way of combining the flexibility of the seal programs with a mandate that all entities that gather consumer information must follow appropriate privacy protections and we are highly supportive of the safe harbor provision.

Chairperson FEINSTEIN. Mr. Comer?

Mr. COMER. I wonder if I might just respond to that, as well.

Chairperson FEINSTEIN. Certainly.

Mr. COMER. We are not only on the board of TRUSTe, but also on the board of BBB Online, and so we have had a very strong voice in working to bring these organizations into existence and strengthen them over the last few years.

I would say we view the safe harbor provisions as not only very well written, but extremely important to the whole schema of the bill, and the reason for that is because you want an incentive that will bring, if you will, the startups, the small businesses, the others that are just learning about privacy responsibility into the self-regulatory organizations because they do an enforcement role which the FTC will never be able to duplicate. They do random checks. They do periodic audits and so forth and that enables the safe harbor programs, the seal programs, excuse me, to be kind of an extended arm of enforcement and compliance.

The way your bill is structured, we think the good players will migrate naturally to those programs in order to benefit from the safe harbor, and in that way, their privacy practices will be sharpened, improved, and better supervised.

Chairperson FEINSTEIN. Mr. Torres? Thank you.

Mr. TORRES. Senator, consumer advocates in general are somewhat wary of the industry's regulating itself. I know that there are some seal programs that are out there today and they were mentioned here today—

Chairperson FEINSTEIN. It seems to me I have heard that before.

Mr. TORRES [continuing]. That are really trying to do the right thing. We fear lack of enforcement as one thing. The other thing is sometimes that you could have a seal program that simply says, if you have a privacy policy, that is what we require, and we know from experience that a company's privacy policy can be fairly hor-

rible and we just want to make sure that those types of seal programs do not get included as part of the program. We would be more than happy to work with your staff on how to make sure there is some oversight, and I think there is some provision for the FTC to take a look at the seal programs that are kind of approved for this purpose.

Chairperson FEINSTEIN. Good. Well, from this point on, I would like to work together to see that the consumer interest as well as the business interests are protected, because when we started this, it was very difficult, as you know. Nobody wanted opt-in in any way, any shape, or any form. So you gentlemen in the business community are really in the forefront of this and I really want to commend you. I am very grateful for this support. I think it is very important that we work together as we make any changes in this that need to be made. I think we have got a pretty good bill that goes as far as it can go.

In looking for points of controversy, one thing may be that we allow for or provide for State enforcement, and one of my reasons is it is the only way the bill is really going to get enforced. You heard the testimony of the GAO, how little the Federal aspect of this has to look into it. So I think the State enforcement of it is extraordinarily important. Do any of you have a view on that?

Mr. COMER. I agree with your view on that because you now have the 50 State attorneys general who will be in a position under this bill to carry forward, if you will, extend the reach of the FTC's jurisdiction and I think the Commission is quite comfortable with that kind of a model. It has been used in COPA and in other pieces of legislation. Provided, as your text is written, that this is subject to the, if you will, the rights of intervenor of the FTC and FTC oversight, we are quite comfortable with State enforcement in this context.

Chairperson FEINSTEIN. Good. Good.

Mr. COMER. I would say it is an equally important part of the preemption provisions that there is no new private right of action created by your bill and that will help keep the law uniform and straightforward with regard to consumer rights.

Chairperson FEINSTEIN. Right. I understand that.

Mr. Avila, do you have a comment?

Mr. AVILA. Yes. We would agree that it is very important that there be a single uniform national standard. The vesting authority in the FTC and in the attorneys general is a very important way to achieve that uniformity.

Chairperson FEINSTEIN. Thank you.

Mr. TORRES. Senator?

Chairperson FEINSTEIN. Certainly. Go ahead.

Mr. TORRES. If I may, on the preemption question, as I said in my testimony, it is crucial, then, that if there is preemption, that the underlying bill be as strong as possible, and your bill is fairly strong on a number of points. And so that for us may be the trade-off. We get preemption thrown at us quite a bit. It undermines a lot of good State efforts in various areas and so that is why I also said in my testimony that we really need to consult with some of the States.

As far as the attorneys general having some enforcement authority here, the attorneys general have done a tremendous job on the issue of privacy both in California and in Minnesota. It was one of the reasons why privacy became such an important part of the Gramm-Leach-Bliley debate, because there were abuses of personal financial information.

So those are just things that we need to be working on through the discussion of this legislation.

Chairperson FEINSTEIN. Thank you very much. I mean, there is no way of doing a bill unless you have preemption because you are going to have different laws in every State and how do you follow that on an online community? You cannot, so it becomes extraordinarily difficult to have any meaningful reform unless you establish that national preemption.

In any event, I think we have done it today. Let me thank you. Ms. Fisher, let me thank you so much for coming this distance to testify and I hope you will work along with the staff to see that victims' rights are protected as we move this legislation along.

It is my intention to have another hearing, I think it is on March 19, and we will consider Senator Cantwell's bill and another bill that Senator Kyl and I have, and then hopefully, if all goes well, maybe combine them into one bill so that we can then move on to the full committee. I would hope that you all would look at those bills, as well, and let us know if you think they are mutually compatible. I appreciate that.

Mr. COMER. Senator, can I just—

Chairperson FEINSTEIN. Senator Thurmond has a statement, which I will put in the record.

We will enter Senator Grassley's statement in the record, as well.

Mr. Comer, did you have a comment?

Mr. COMER. A final comment. I want to thank your staff for their very fine work and working closely with us to polish some of the provisions.

Chairperson FEINSTEIN. Thank you very much.

Mr. TORRES. I second that.

Chairperson FEINSTEIN. And Senator, thank you very much, and I particularly appreciate that. It has been a lot of work.

Let me thank the witnesses. The hearing is adjourned.

[Whereupon, at 4:38 p.m., the subcommittee was adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

AMERICAN ELECTRONICS ASSOCIATION
WASHINGTON, D.C.20004
February 12, 2002

The Hon. Dianne Feinstein
U.S. Senate
331 Hart Building
Washington, DC 20510

Dear Senator Feinstein:

Thank you for your ongoing leadership on the very important issue of privacy. AeA has a significant interest in "The Privacy Act of 2001" (S. 1055). I write in support of the essential elements of Title I of this bill. While we have concerns about other titles of the bill, we do want to express our commitment to work with you in your efforts to strengthen protections for consumer privacy on the Internet

As you know, AeA is the largest high-technology trade .association in America, representing over 3,500 companies that develop and manufacture software, electronics, and high technology products. Our member companies range from large, industry leaders to small and medium sized high-technology start up ventures. As such, online consumer confidence is of paramount concern to AeA members. Furthermore, many AeA companies use information gathered from their customers to alert them to new products and services that may be useful in their homes or offices. The proper use of this information is essential to the growth of the Internet economy. Therefore, any attempt to regulate information practices must be approached with caution and only after careful consideration of the potential unintended consequences of such regulation.

It is important to emphasize that our current support for federal preemption legislation is a direct response to the multiplicity of state privacy initiatives that were considered during 2000 and 2001. AeA believes that patchwork state regulation will reduce consumer confidence online by presenting consumers with conflicting privacy protections, as well as harm small and medium sized businesses by forcing them to comply with a multiplicity of regulations. Also, we continue to believe that industry self-regulatory efforts must play a significant role in any federal proposals.

AeA's Board has approved principles for federal legislation that are set forth at the end of this letter. Fundamental to these principles are the benchmarks of notice, choice, and uniform federal standards for privacy protection. We are very pleased that Title I of your bill includes clear notice and choice provisions consistent with our principles, as well as a strong federal preemption section that would provide certainty for both consumers and businesses about their respective rights and responsibilities. Importantly, your bill would also apply these same requirements to offline data collection activities. This is consistent with our principle that policy should not discriminate between online and offline activities to the disadvantage of e-commerce.

We stand ready to work productively with you to maintain the proper balance between the need to strengthen protections for consumers while avoiding unnecessary restrictions on the ability of businesses to provide, through the Internet, the valuable products and services that consumers demand.

Sincerely,

WILLIAM T. ARCHEY
President & CEO

AEA PRINCIPLES FOR INTERNET PRIVACY LEGISLATION

PROVIDE INDIVIDUALS WITH NOTICE

Web sites that collect personally identifiable information should provide individuals with clear and conspicuous notice of their information practices at the time of information collection. Individuals should be notified as to what type of information is collected about them, how the information will be used, and whether the information will be transferred to unrelated third parties.

ENSURE CONSUMER CHOICE

Consumers should have the opportunity to opt out of the use or disclosure of their personally identifiable information for purposes that are unrelated to the purpose

for which it was originally collected. Consumers should be allowed to receive benefits and services from vendors in exchange for the use of information. It is important that the consumer understands this use and be able to make an informed choice to provide information in return for the benefit received.

LEVERAGE MARKET SOLUTIONS

Private sector privacy codes and seal programs are an effective means of protecting individuals' privacy. Lawmakers should recognize and build upon the self-regulatory mechanisms the private sector has put in place and continues to build. These mechanisms are backed by the enforcement authority of the Federal Trade Commission and state attorneys general. Public policies also should allow organizations to implement fair information practices flexibly across different mediums and encourage innovation and privacy enhancing technologies.

ENSURE NATIONAL STANDARDS

The Internet is a new and powerful tool of interstate commerce. Public policies related to Internet privacy should be national in scope, thus avoiding a patchwork of state and local mandates. This uniform framework will promote the growth of interstate ecommerce, minimize compliance burdens, sustain a national marketplace and make it easier for consumers to protect their privacy.

PROTECT CONSUMERS IN THE PUBLIC AND PRIVATE ARENA

Government and non-profit organizations collect a tremendous amount of personally identifiable information about citizens. The need to foster consumer confidence applies to private and public sector activities. Government agencies and non-profit organizations that collect personally identifiable information should be required to follow fair information practices imposed on the private sector by law or regulation.

DON'T DISCRIMINATE AGAINST THE INTERNET

Consumers should have confidence that their privacy will be respected regardless of the medium used. Similar privacy principles should apply online and offline. Public policy should not discriminate against electronic commerce by placing unique regulatory burdens on Internet-based activities.

UTILIZE EXISTING ENFORCEMENT AUTHORITY

With the imposition of notice requirements, the Federal Trade Commission should use its existing authority to enforce the mandates of federal legislation. Legislation should not create any new private rights of action.

AVOID CONFLICTING OR DUPLICATIVE STANDARDS

In cases where more than one government agency seeks to regulate the privacy practices of a particular organization or industry, those agencies should offer a single coordinated set of standards.

Statement of American Medical Association

The American Medical Association (AMA) and its physician and medical student members appreciate the opportunity to present information to this Subcommittee on the important issue of patient privacy and the confidentiality of medical records. The AMA believes that patient privacy is fundamental to the physician-patient relationship and is a right long advocated by the AMA.

We would like to commend Chairman Feinstein for introducing S. 1055, the "Privacy Act of 2001." Title IV of S. 1055 would significantly improve the current framework of federal privacy protections for all of America's patients.

BACKGROUND ON FEDERAL PRIVACY PROTECTIONS

The Department of Health and Human Services (HHS) published on December 28, 2000, a final rule establishing standards for the privacy of individually identifiable health information ("Standards for Privacy of Individually Identifiable Health Information" 65 Fed. Reg. 82462) (the "Final Privacy Rule "). Congress did not pass privacy legislation by the August of 1999 deadline set by the Health Insurance Port-

ability and Accountability Act of 1996 (HIPAA). Therefore, the Secretary of HHS issued privacy standards as directed by HIPAA.

The AMA applauds HHS for the tremendous effort it took to write the Final Privacy Rule. After years of contentious debate in Congress it became clear to all involved that drafting federal privacy standards would be no easy task. Overall, the AMA is pleased with many provisions of the Final Privacy Rule. However, we also have many serious concerns.

During a public comment period in March of 2001, the AMA submitted extensive comments on the Final Privacy Rule. Among many significant issues, we expressed concern over the marketing provisions. We also expressed concern that, even with potential future improvements, the Final Privacy Rule would not adequately protect patients because it only applies to certain "covered entities." We firmly believe that Congress must act to extend privacy requirements to all entities that maintain patient information.

Because HIPAA limited the Secretary's regulatory authority to health care providers, health plans, and health data clearinghouses, these are the only entities covered under the Final Privacy Rule. All other users of individually identifiable health information ("protected health information ") are not regulated by the Final Privacy Rule. Yet, protected health information is received by many other entities such as schools and universities, public and private agencies that oversee health care treatment and payment, law enforcement officials, and public health departments. These entities include, but are not limited to, state insurance commissioners, state health professional licensure agencies, the Office of Inspectors General of federal agencies, the Department of Justice, State Medicaid fraud units, Defense Criminal Investigative Services, the Pension and Welfare Benefit Administration, the HHS Office for Civil Rights, the Food and Drug Administration, the Social Security Administration, the Department of Education, the Occupational Health and Safety Administration, and the Environmental Protection Agency.

Other persons or entities may also receive protected health information in the normal course of business such as lawyers, accountants, consultants, etc. The Final Privacy Rule identifies such secondary users of protected health information as "business associates" of physicians and other covered entities. The Final Privacy Rule requires that the confidentiality standards of the rule be applied to these business associates through contracts with covered entities.

The AMA objects to the business associate provisions because they present the potential for significant liability for physicians even when the physicians themselves are in compliance with the Final Privacy Rule. Covered entities are subject to enforcement and sanctions under the Final Privacy Rule for acts of their business associates, while business associates at most may lose their contract with the covered entity and incur possible damages if the covered entity files a subsequent civil suit. In addition, covered entities will have a duty to mitigate any known harmful effects of a violation of the rule by a business associate.

As currently written, the business associate requirement will subject physicians and covered entities to an array of both foreseeable and unforeseeable compliance costs. All existing contracts with each business associate will need to be rewritten and renegotiated. Every single interaction physicians have that might involve the disclosure of protected health information will require analysis. For example, state and county medical associations that assist physicians with specific compliance, patient care and billing issues, as well as private accreditation and certification agencies, will now be required to have business associate contracts.

The AMA acknowledges the limitations inherent in the Congressional grant of authority under HIPAA that constrain the Secretary from directly regulating secondary or "downstream" users of protected health information. However, covered entities should not be held responsible for actions taken or inaction by these separate entities simply because Congress did not include them in the legislative directive to HHS. As a matter of fairness, these users of protected health information should also be brought under the terms of comprehensive privacy laws.

Fortunately, Chairman Feinstein has taken a first step to address these concerns.

Title IV of S. 1055 would prohibit the unauthorized sale of protected health information by entities that maintain protected health information but are not "covered entities" under the privacy regulation. S. 1055 would also remove harmful marketing loopholes from the Final Privacy Rule. These are two much needed improvements to federal privacy protections.

THE SALE OF HEALTH INFORMATION

The AMA is pleased that Title IV of S. 1055 would expand federal privacy protections for patients by establishing some conditions on the disclosure of protected

health information received and maintained by entities that are not covered under the Final Privacy Rule. Title IV would prohibit these "non-covered entities" from selling protected health information without an authorization by the patient. "Non-covered entities" under S. 1055 would include all public or private entities such as health researchers, schools and universities, life insurers, property and casualty insurers, employers, public health authorities, health oversight agencies, law enforcement officials, and any person acting as an agent of such entities.

In addition, S. 1055 would ensure that patients are adequately informed before they authorize the sale of their protected health information. Authorizations would need to be in writing, explain the purpose for which the information would be sold, identify in a specific and meaningful manner what information would be sold, the persons who would be selling the information, and the persons who would receive the information. Individuals would also have the right to revoke an authorization and entities would not be permitted to condition the purchase of a product or service on an individual signing an authorization.

We would like to voice one cautionary note, however, regarding the definition of "sale." Because it could, and should, be interpreted very broadly, the definition of "sale" might lead to the unintended consequence of prohibiting important research, particularly research published in medical journals. Without a clarification, we are concerned that the use of protected health information for analysis and research that is later published might be considered to be an "indirect" sale of protected health information under Title IV of S. 1055. We would like to propose a rule of construction for addition to the language of the bill that would address this matter.

MARKETING

In the Final Privacy Rule, marketing is defined very broadly as "mak[ing] a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service." There is a "carve out" for certain oral communications and written communications if the covered entity does not receive remuneration from a third party for making such a communication. These communications are not considered marketing if they are made by a health care provider and tailored to a particular patient as part of treatment, or made by a provider or plan to manage treatment of a patient or recommend alternative therapies, providers, or settings of care. S. 1055 maintains this appropriate definition.

The proposed privacy rule included a general prohibition against the use of protected health information for marketing without a patient authorization and would have prohibited the disclosure of such health information for sale, rental or barter without patient authorization. However, these prohibitions were weakened in the final rule. The Final Privacy Rule removed altogether the prohibition against disclosure of protected health information for sale, rental or barter without patient authorization. And, although patient authorization for marketing of protected health information is still required, there are several exceptions that effectively remove this protection in many circumstances. (Section 164.514(e)(1)) This is unacceptable to the AMA.

Under the Final Privacy Rule, the marketing communications that are exempt from the authorization requirement fall under the definition of "health care operations." Health care providers are required to obtain patient consent before protected health information can be used or disclosed for health care operations under the Final Privacy Rule.

But, for health plans, this is a major loophole because they do not need to obtain patient consent to conduct health care operations under the Final Privacy Rule. This means health plans can use or disclose protected health information for various marketing purposes without any type of permission from the patient.

The Final Privacy Rule exempts from the authorization requirement communications that occur in a face-to-face encounter with the individual but it is not limited to those between physicians and patients. Therefore, any face to face encounter on behalf of a covered entity is excluded from the authorization requirement. This could potentially include telemarketing, or door to door marketing of items or services unrelated to health care.

The Final Privacy Rule also exempts from the authorization requirement items and services of nominal value. This overly broad exception is unacceptable to the AMA. "Nominal value" a vague term that could include all kinds of marketing communications to patients. This exception also allows the use of protected health information without patient authorization for marketing items or services that are not even health related.

Another exception under the Final Privacy Rule permits marketing of health-related items and services on behalf of third parties (pursuant to a business associate contract). The marketing communication must identify the covered entity as the party making the communication, state whether any remuneration was received, and allow the patient to opt-out from future communications. Therefore, a health plan or pharmacy can sell a patient list without the patients' authorization to a pharmaceutical company or pharmaceutical benefits manager (PBM) as long as a business associate contract is in place. The pharmaceutical company or PBM can then send the patients information about prescription drugs that are alternatives to their current prescriptions. This will offend many patients as an unwanted intrusion into their personal health. The AMA has heard that many patients are already complaining to their physicians about receiving such marketing communications at home.

The opt-out requirement in the Final Privacy Rule is also weak and full of loopholes. No opt-out procedure is specified in the rule and covered entities must only make "reasonable efforts" to ensure that those individuals who opt-out from future marketing communications do not receive another such communication. Therefore any type of opt-out process is permitted, even one that is extremely inconvenient to the patient. There is no opt-out requirement when the marketing communication is sent to a broad cross-section of patients or enrollees.

We strongly support the provisions of Title IV of S. 1055 that would eliminate these harmful marketing exceptions from the Final Privacy Rule. In addition, Title IV of S. 1055 would expand the protections in the Final Privacy Rule by extending the prohibition from using, disclosing, or selling protected health information for marketing without patient authorization to non-covered entities as well. These are two much needed improvements to federal privacy protections.

CONCLUSION

The AMA commends Chairman Feinstein for including Title IV in S. 1055, the "Privacy Act of 2001." The provisions of Title IV would strengthen the Final Privacy Rule by removing harmful marketing loopholes and would extend federal privacy protections beyond the coverage of the Final Privacy Rule by prohibiting all entities that maintain protected health information from selling or marketing such information without the approval of the patient.

The AMA strongly supports Title IV of S. 1055 as a step in the right direction for America's patients. We also encourage Congress to consider additional legislation to further improve the Final Privacy Rule and to further extend the coverage of privacy protections to all entities that maintain health information. As the President acknowledged on Monday during remarks to physicians in Wisconsin: "personal medical information must always be strictly confidential. A patient's right to privacy must be protected." [Emphasis added.]

We look forward to working with the Subcommittee on this and other important privacy legislation.

Statement of Hon. Charles E. Grassley, a U.S. Senator from the State of Iowa

Madam Chairwoman and Senator Kyl, thank you for allowing me to make a few comments on this important matter. As you know, I'm no longer a member of this Subcommittee, but I remain very interested in making sure that we eradicate identity theft. So I thank the Chair for her indulgence.

The dangers to our society and its citizens that result from the misuse of personal information are significant. Social Security Number misuse is a subset of identity theft. This pervasive use of SSNs coupled with the advent of the Internet has opened up new opportunities for wrongdoers to create false identities. And we've all seen that when a person's name and other identifying information is stolen to commit theft or fraud, or to access confidential information, there can be devastating results. The Inspector General of the Social Security Administration reported that, "The tragedies of [September 11] demonstrate that SSN misuse and identity theft are breeder' offenses with the ability to facilitate crimes beyond our imagination." We now know that identity theft was a prime modus operandi of the terrorists. The hijackers and their suspected accomplices committed identity theft, including at least one documented case of using a false Social Security Number, to infiltrate American society while planning these attacks.

Congress can help make it a lot harder for these criminals to get this sensitive information. There are a number of bills currently pending in Congress that try to do just that. I've joined with Senators Feinstein and Kyl in sponsoring "The Identity Theft Prevention Act of 2001" to make it more difficult to steal someone's identity, and to impose additional duties on credit issuers and credit bureaus to ensure the accuracy of information in credit applications.

Let me say just a few words about some relevant data that my Finance Committee investigative staff has found with respect to the safeguarding of SSNs by the Social Security Administration and the Department of Veterans Affairs. The Inspector General of the Social Security Administration reported that SSA has no programs designed to uncover illegal activity or to assist in the detection of terrorist activity. According to the Inspector General, "Once an individual obtains an SSN, either through proper or improper means, the Agency has little ability to control the use of that, number." SSA controls to detect or prevent undocumented immigrants from obtaining a false or stolen SSN "do not always work as intended and are not always used." This is not good enough. Knowing what we know now about the 9–11 terrorists, the Social Security Administration's safeguarding of Social Security Numbers must be among its highest priorities.

The Department of Veterans Affairs didn't fare much better in terms of improper access to and theft of Social Security Numbers. I asked the Inspector General to examine cases involving identity theft by VA employees, patients or visitors. The Inspector General found losses to the VA to include:

- $11.5 million in improper benefit payments;
- $52,000 in fraudulent credit card charges; and
- $159,000 worth of medical treatment.

This supports the Inspector General's finding that, "VA programs and operations have identified a continuing vulnerability to destruction, manipulation, use, and inappropriate disclosure of sensitive veteran identifier information." Although there are levels of access, once employee access is assigned, "restrictions have not been implemented to prevent full access to all veterans" information in that group." That information may include Social Security Numbers and :medical histories of psychosis or other mental ailments. I think this is very troubling.

Clearly, these agencies, as well as other federal agencies, need to reform their programs to identify and combat Social Security Number misuse, and I intend to help them with this effort. But the federal agencies cannot do it alone. As people increasingly rely on credit cards for electronic commerce and daily business transactions, industry needs to step up to the plate to protect consumers' sensitive information. And Congress can enact tougher laws that make it harder for these criminals to obtain access to this information, and that severely penalize identity thieves. I hope we can minimize opportunities for invasions of privacy in the form of identity theft through legislative and oversight initiatives. The American people deserve no less than knowing that their identities are protected.

Statement of Hon. Orrin G. Hatch, a U.S. Senator from the State of Utah

Madame Chairwoman, I want to thank you for holding this important hearing. As we recently have been made acutely aware, identity theft has become one of the most critical tools of the criminal trade of terrorists as well as other criminals. In this information age, identity theft is one of the fastest growing crimes in the United States. Of the 204,000 consumer fraud complaints compiled by the Federal Trade Commission last year, 42% involved identity theft. Recent news reports suggest that as many as 750,000 identities are stolen each year.

This Subcommittee is well aware of how criminals appropriate personally identifiable information, including Social Security numbers, to steal money, credit records, victims' good names, and, in some cases, to commit violent crimes. As a result, victims incur substantial harms, including financial losses, damaged credit histories, and legal problems, which take long periods of time to rectify.

In 1997, Senator Kyl introduced "The Identity Theft and Assumption Deterrence Act." Together we worked with our House counterparts to enact this bill into law. Among other things, the Act made it a crime to transfer or use, without lawful authority, a person's means of identification, including a Social Security number, with the intent to commit a violation of Federal law, or a felony under State or local law.

"The Identity Theft and Assumption Deterrence Act" represented an essential first step in our effort to curb identity theft. But we can, and should, consider additional preventive measures to reduce this pervasive problem. In so doing, however,

we must be careful to ensure that such legal reforms do not unduly restrict businesses and financial institutions in their legitimate commercial dealings.

I applaud Senator Feinstein's effort to develop legislation that attempts to balance the privacy rights of consumers with the needs of this nation's businesses, and I am committed to working with her and this Subcommittee to strike the proper balance between these important interests. I look forward to hearing from our distinguished witnesses.

Statement of Jeff P. Nicol, Customer Privacy Manager, e-Business Group, Intel Corporation

INTEL PRIVACY PERSPECTIVE

Thank you for giving me the opportunity to speak before you today. My name is Jeff Nicol and I manage the Privacy Compliance Team at Intel Corporation. Intel supplies computer chips, boards, systems, software, networking and communications equipment, and services that comprise the "ingredients" of computer architecture and the Internet. Intel's mission is to be the preeminent building block supplier to the worldwide Internet economy.

Let me give you some background on how Intel got so involved in the privacy debate. In late 1998, we disclosed our plans to include a serial number feature in the next version of our flagship microprocessor. Almost immediately, some end users and privacy advocates told us that such a feature was a threat to their privacy. Our intention in developing the feature had been to find a simple technical solution to our clients' request to provide greater security for private information through stronger identification tools. Unfortunately, what we perceived to be a technical issue raised privacy concerns for many end users. We quickly took steps to provide greater control of this feature for users. We realized that the best way to satisfy consumer concerns in an environment of heightened anxieties is to clearly disclose your personal information collection & handling practices and offer people the ability to exercise choices regarding those practices.

Our privacy program has come a long way since its rough and tumble beginning. We established a three-tiered organization structure to manage our privacy programs. At the top is an executive staff led Management Review Committee. Management Review Committee membership includes our General Counsel, Chief Information Officer, and the Vice President of Marketing. This senior management backing gives our program top-down support as well as bottoms-up visibility. Next, we have the Privacy Compliance Core Team (which I lead). My team deals with the day-to-day responsibilities of setting, implementing, and enforcing our policies. This takes the fulltime efforts of four of us, plus we receive a tremendous amount of support from employees across the corporation. Lastly, we have the Privacy Review Board. The Privacy Review Board is a cross-functional team comprised of the Privacy Compliance Core Team, plus subject area experts in fields such as Law, Information Security, Human Resources, Information Technology, Customer Support, and other disciplines. The Privacy Review Board is a balanced forum in which employees may raise questions related to the privacy implications of new technologies and services or interpretation of existing privacy policies.

In addition to our internal compliance efforts, we have many externally visible accomplishments. In the self-regulatory space, we are founding sponsors of both BBBOnLine and TRUSTe, and are proud holders of their respective privacy seals. We continue to actively support these groups, especially in the area of helping them expand their programs internationally. Continuing with the international theme, Intel filed for Safe Harbor Certification with the US Department of Commerce in June. This certification provides us with a uniform mechanism for compliance with the European Union (EU) Data Protection Directive for our online and offline customer data. Lastly, on the technology front, we have been working with the World Wide Web Consortium (W3C) on rolling out the Platform for Privacy Preferences (P3P) technology. P3P provides an automated way for users to gain more control over the use of personal information on Web sites they visit. Intel sites will all be P3P compliant.

While some privacy technologies (like P3P) are promising, they only offer part of a solution and are not a substitute for federal privacy legislation. Members of this Committee may be aware that Intel has taken a proactive stance within our industry associations, such as AEA, CompTIA, and ITI, in favor of the passage of federal Internet privacy legislation. I will touch on the principles that should guide such

legislation in a moment, but first I would like to comment on the reasons why we believe Congressional ground rules are required.

WHY CONGRESSIONAL GUIDANCE IS NECESSARY

First, we are persuaded that there is a general level of uncertainty on the part of consumers regarding the safety of doing business on the Internet that has been a major factor restraining the growth of consumer commercial transactions. While the general public has embraced the Net as a ready source of information and a tool for communications, and businesses are aggressively adopting e-business models, the average consumer is reluctant to purchase products or services through the Internet. A recent Gartner survey of 7,000 consumers showed that 60% say security and privacy concerns keep them from doing business online.1In our judgment, privacy is one of the key consumer concerns that hold that percentage down. Congressionally mandated "ground rules" will go a long way toward alleviating these concerns. Consumers need to have confidence no matter what state they live in. They should not be left guessing to what degree they are protected when they move from state to state.

Second, there is the need to educate businesses. Intel has been proactive in the Privacy Leadership Initiative (PLI), which has ardently advocated the adoption of fair privacy practices by firms doing business on the Internet. The adoption of fair privacy practices is well advanced in the community of large, Fortune 500 level business entities; but in the world of start-ups, new entrants to the Internet space, and small business in general, the record is not as good. There are problems with awareness of best industry practices, compliance with articulated policies when dealing with outside parties, and responsible internal management of data. Again, we think that federally mandated rules on basics such as notice and choice would focus business attention at all levels and raise the level of consumer protection.

Third, there is the issue of doing business in Europe. As members may be aware, the U.S. and the European Union reached a landmark agreement in calendar year 2000, commonly known as the "Safe Harbor" agreement. This agreement, negotiated by the U.S. Department of Commerce, provides framework through which U.S. companies may certify compliance to European data privacy and security requirements and collect data from consumers in EU countries with a presumption of compliance with European directives governing the collection and use of information. During negotiations, European negotiators raised strong concerns regarding the availability of enforcement tools in U.S. law. In response to those concerns, the agreement's drafters referenced provisions of the Federal Trade laws that grant the Federal Trade Commission (FTC) the power to regulate, and punish, companies for making misleading, false or fraudulent statements to consumers in connection with the sale of goods and services. While the EU has accepted for now that existing FTC powers provide a "floor" level of enforcement authority, the continued viability of this agreement may in large part be dependent on whether the U.S. moves, over time, to strengthen consumer rights and the oversight role of federal authorities. The EU Safe Harbor agreement is critical to the stability and predictability of the Internet business environment in Europe.

Finally, if one concludes as we at Intel have that strengthening consumer rights is necessary, it is apparent that those rights, as well as the rights and responsibilities of businesses, should not vary from state to state. Our Chairman, Dr. Andy Grove, believes personal data has value and therefore, consumers have legitimate property rights regarding their personally identifiable information. Over time, legislatures will act to define and recognize the legal status of those property rights. Today, there are numerous bills pending in state legislatures all over the United States most actively in California, Delaware, Massachusetts, and New York that would mandate specific practices with respect to the handling of consumer data or the design and management of websites. A scenario where those rights and responsibilities varied from state to state would sow confusion, uneven enforcement of rights, and a threat of legal liability in multiple states under multiple standards. Such an environment would retard the growth of e-commerce in the consumer space for years to come.

PRINCIPLES THAT SHOULD GUIDE CONGRESS

For all of these reasons, we believe that the time has come for Congress to act. Now I would like to comment specifically on what we believe Congress can, and should, do that will enhance consumer rights, help build the Internet into a powerful tool of interstate commerce for consumers, and provide guidance for industry regarding privacy policy.

All of the major high-tech industry associations to which we belong have articulated core principles that should guide privacy legislation. In sum, these principles though not detailed prescriptions of legislative language provide a template for sound policy choices. I will reference the statement of principles adopted in January of 2001 by the American Electronics Association (AeA) as perhaps the best example of the thinking within our industry.

AeA guidelines, adopted to put "flesh on the bones" of a Board resolution in favor of preemptive federal privacy legislation, address seven substantive areas: notice, choice, the appropriate role of the private sector, the need for national standards, application of those standards to both public and private websites, treatment of off-line data collection on the same basis as on-line collection activity, appropriate enforcement mechanisms, and avoiding duplicative requirements for specific industry sectors. The guidelines state as follows:

AEA GUIDELINES REGARDING COMPUTER PRIVACY

Provide Individuals with Notice

Web sites that collect personally identifiable information should provide individuals with clear and conspicuous notice of their information practices at the time of information collection. Individuals should be notified as to what type of information is collected about them, how the information will be used, and whether the information will be transferred to unrelated third parties.

Ensure Consumer Choice

Consumers should have the opportunity to opt-out of the use or disclosure of their personally identifiable information for purposes that are unrelated to the purpose for which it was originally collected. Consumers should be allowed to receive benefits and services from vendors in exchange for the use of information. It is important that the consumer understands this use and is able to make an informed choice to provide information in return for the benefit received.

Market Solutions

Private sector privacy codes and seal programs are an effective means of protecting individuals' privacy. Lawmakers should recognize and build upon the self-regulatory mechanisms the private sector has put in place and continues to build. These mechanisms are backed by the enforcement authority of the Federal Trade Commission and state Attorneys General. Public policies also should allow organizations to implement fair information practices flexibly across different mediums and encourage innovation and privacy enhancing technologies.

Ensure National Standards

The Internet is a new and powerful tool of interstate commerce. Public policies related to Internet privacy should be national in scope, thus avoiding a patchwork of state and local mandates. This uniform framework will promote the growth of interstate e-commerce, minimize compliance burdens, sustain a national marketplace and make it easier for consumers to protect their privacy.

Protect Consumers in the Public and Private Arena

Government and non-profit organizations collect a tremendous amount of personally identifiable information about citizens. The need to foster consumer confidence applies to private and public sector activities. Government agencies and non-profit organizations that collect personally identifiable information should be required to follow fair information practices imposed on the private sector by law or regulation.

Don't Discriminate Against the Internet

Consumers should have confidence that their privacy will be respected regardless of the medium used. Similar privacy principles should apply online and offline. Public policy should not discriminate against electronic commerce by placing unique regulatory burdens on Internet- based activities.

Utilize Existing Enforcement Authority

With the imposition of notice requirements, the Federal Trade Commission should use its existing authority to enforce the mandates of federal legislation. Legislation should not create any new private rights of action.

Avoid Conflicting or Duplicative Standards

In cases where more than one government agency seeks to regulate the privacy practices of a particular organization or industry, those agencies should offer a single coordinated set of standards.

We believe these guidelines lay out a path for Congressional policy that is coherent, logical and addresses the core concerns of consumers and the needs of business for predictability and stability in the legal environment.

Title I of S. 1055 Is Consonant with AeA Guidelines and Advances Consumer Rights

S. 1055 is a comprehensive attempt to speak to a wide variety of concerns regarding the proper collection and use of consumer information in many different social contexts. While we will leave to others the merits of specific provisions dealing with identity theft, financial and health information, we applaud you, Chairman Feinstein, for your efforts to focus Congress' attention on the need for a systemic approach to the variety of privacy issues facing consumers. With regard to Internet privacy—an area where we do have expertise I am pleased to state that Intel strongly supports the provisions of Title I of your bill. They would substantially strengthen the ability of Internet users to protect their privacy in a manner consonant with the industry guidelines that we support.

Ensuring that an Internet user has clear and conspicuous notice of information collection and disclosure or sale practices, and the opportunity to exercise choice regarding the collection and use of user information, is the essential foundation of protecting privacy. Your bill would achieve this, and it would moreover provide for effective enforcement of such rights through the auspices of the FTC and state Attorneys General. This federal/state enforcement structure will help guarantee that the rights of users are the same no matter where the user or the website is located, and it is supplemented by a strong preemption provision that will guarantee uniformity of rights across state boundaries. Uniformity of rights is accomplished by language in your bill that clearly establishes the primary role of the FTC in shaping implementation rules, forecloses conflicting state statutory and regulatory law, and common law. It creates no new private right of action which is a critical point for our industry and gives the FTC the authority to intervene in enforcement actions brought by state authorities. Consumers will have the benefit of uniform rules throughout the nation, enforcement of those rules by federal and state authorities, and businesses will have clear and straightforward obligations established by one authority.

Equally important, however, are the safe harbor provisions of your bill that will minimize legal uncertainties for businesses participating in voluntary trust seal organizations such as BBBOnLine and TRUSTe. These seal organizations serve the important function of certifying member companies' adherence to fair privacy practices, and their efforts to recruit participation of companies will also be strengthened by your bill should it be enacted into law.

Title I of S. 1055 applies to both on-line and off-line data collection activities, ensures segregation of general on-line standards from requirements already established for health and financial data, and establishes reasonable penalties for flagrant violations. We would like to see the notice and choice requirements of S. 1055 extended generally to public sector web sites, and we believe that a further requirement of independent verification of compliance to policies should be articulated in statute to provide stronger "teeth" for self-regulatory efforts. We would be pleased to offer specific legislative language suggestions to the Committee toward those ends if desired.

In sum, we believe that the continuing viability of the Internet marketplace depends upon good rules, good practices, and good policing. Congress should lay down the rules, depend upon the self-regulatory tools now in the marketplace to advance the adoption of fair privacy practices, and give responsibility for the enforcement of those rules to the FTC and state Attorneys General. In this way, bad actors will—over time—be driven out of the marketplace and consumer acceptance of the Internet as a safe place to do business will be secured. The Internet will flourish as one of the most efficient, if not the most efficient, market tools ever developed.

On behalf of the senior executives of Intel, and our entire privacy team, I thank you Senator Feinstein for your leadership on the important issue of Internet privacy. We pledge to work with you and other members of the Congress to secure the privacy rights of Internet users through balanced federal legislation such as Title I of S. 1055.

Thank you for your time. I will be pleased to answer any questions you may have.

Statement of Laura Nyquist, Chief Privacy Officer, NCR Corporation

Chairwoman Feinstein, Senator Kyl, and members of the Subcommittee, my name is Laura Nyquist, Chief Privacy Officer for NCR Corporation. Thank you for the invitation to submit written testimony today before your Subcommittee.

As the Chief Privacy Officer, I supervise compliance across all NCR's businesses to the company's privacy policy and international privacy laws, as well as oversee the company's privacy initiatives implemented in the solutions we provide to our customers. As you may know, NCR was an early leader in the privacy space as our Teradata database was the first to incorporate consumer data protection.

NCR's heritage in providing solutions for the retail industry goes back over 115 years when it was founded as the National Cash Register Company in Dayton, Ohio. Now NCR Corporation is one of the world's largest suppliers of solutions that facilitate and optimize transactions between consumers and businesses, whether in stores, through self-service equipment, or over the Internet. NCR currently employs over 31,000 people globally.

Madame Chairwoman, the subject of today's hearing is important to us all, as we are all consumers.

Businesses collecting information about their customers is not new. Your grandmother's butcher probably knew not only her name and her favorite cuts of meat, but how the children were doing in school as well. We used to call it "friendly, personal service" at a time when businessmen and their customers were also neighbors.

Today, technology makes it possible for companies thousands of miles away to also serve their customers better by collecting and using massive amounts of data. This explosive growth in data collecting is fueling the global debate over privacy; creating a tension between consumers' sharing of personal information and businesses attempting to realize competitive advantage from gathering and analyzing personal data to better and more efficiently serve them.

A division of NCR called Teradata provides data warehousing and customer relationship management solutions to a wide range of businesses and industries. Our Teradata customers include 20 of the world's largest retailers, 19 of the world's largest banks, 10 of the largest global telecommunications companies, 8 of the world's leading airlines and 10 of the largest insurance companies. Simply stated, NCR provides companies with the technology to strengthen their relationships with customers in ways that protect their privacy and earn their trust. Again, ensuring privacy is essential to building trust that, in turn, is needed to build enduring customer relationships and customer loyalty.

The benefits to consumers of targeted, one-to-one marketing and the protection of their personal data are not incompatible; consumers should and must have control over the use of their personal data.

Surveys show that consumers will gladly provide personal information if they perceive a worthwhile benefit. A recent study shows how American consumers view privacy on the Internet-54% of them routinely give personal information to web sites and an additional 10% would be willing to provide the same information under the right circumstances.

Privacy, the protection and appropriate use of personal information, is a growing concern for consumers and businesses. To ensure continued business success and growth, it's important for companies, big and small, to address privacy as an increasingly important consumer expectation.

One fundamental necessity of commerce, both online and offline, both traditional as well as e-commerce, is trust. Without trust, businesses cannot survive. Businesses and, for that matter, government entities—that do not heed the privacy concerns of their customers will quickly lose trust, and ultimately their ongoing viability.

Customers in control of their data may freely choose release of their personal information in return for better choices or services. I would suspect that you as an airline passenger would not mind being offered an upgrade at the gate because the airline agent knows you experienced a flight cancellation days earlier.

Most companies are doing the right thing in providing privacy options. But as long as there is potential short-term gain in abusing personal information, can we count on company voluntarism to prevent abuse? While many company executives shudder at the thought of more regulation, their companies and customers alike will be better served if industry and government work together toward rational and uniform rules that are fair to all. NCR believes that reasonable legislation is needed to ensure that there are universal controls on the collection and use of personal

data. The right legislation built on top of market-driven solutions can assure that all companies provide this protection.

There are currently laws which impact specific industry sectors such as telecommunications, financial services and healthcare. Additionally, State legislatures are debating various privacy bills that will further complicate this matter. But in the U.S. there is currently no single, broad- based law that affects personal data collection and use, which is why we are here today.

But what type of legislation can work? First, it must be comprehensive and apply the same privacy requirements to all personal data, whether collected online, over the telephone or in face-to-face commercial transactions. It would be misleading to American consumers to enact legislation that applies only to online activities. As a supplier of business intelligence solutions, NCR knows that click-and-mortar firms do not distinguish between personal data obtained through different channels. Online transactions account for only a small fraction of consumer transactions. Last year, online sales accounted for less than one percent of all retail business. Further, the movement of the Internet to the wireless world, the integration of Internet sales channels with Customer Call Centers, and voice-actuated Internet services are blurring the distinction between on-line and off-line.

Obviously, any law that addresses only online transactions limits the benefit to the consumers compared to one that equally addresses online and offline activities. Simply put, data is data.

Madame Chairwoman, I am proud to say that your bill, S. 1055 accomplishes this goal. It accurately addresses the needs of consumers and businesses. S. 1055 ensures that clear and conspicuous disclosures are made about privacy practices and enables individuals to make informed choices about sharing their personal information. Title I of your bill addresses personal data protection in commercial transactions and is written in a comprehensive and effective manner.

During NCR's long business history, a lot of things have changed, but its philosophy has not if you want your customers' trust, you have to respect your customers' privacy. In summary, NCR is pro-privacy. S. 1055 is a step in the right direction and I look forward to working with the members of this Subcommittee on enacting good privacy legislation. The business of privacy is quite simply, good business.

Madame Chairwoman, thank you for holding this hearing today and thank you for your hard work on drafting S. 1055. This is a very complicated and difficult issue and you are to be commended for your interest in moving this important matter forward.

Statement of Evan Hendricks, Editor/Publisher, Privacy Times, Washington, D.C.

Madame Chairwoman, thank you for the opportunity to testify before the Subcommittee. My name is Evan Hendricks, Editor & Publisher of Privacy Times, a Washington newsletter since 1981. For the past 24 years, I have studied, reported on and published a wide range of privacy issues, including credit, medical, employment, Internet, communications and government records. I have authored books about privacy and the Freedom of Information Act. I have been qualified by the Federal courts as an expert in Fair Credit Reporting Act and identity theft litigation. I have served as an expert consultant for government agencies and corporations. I am also a founding member of the Privacy Coalition, which consists of the nation's leading consumer and privacy advocates.

Madame Chairwoman, from the outset, I want to express support in the strongest possible terms for your leadership. To the best of my knowledge, you have taken one of the most comprehensive approaches to privacy of any Member of Congress. This is crucial because privacy is a far-reaching issue, one that touches all aspects of our society. Only a comprehensive approach will begin to confront the challenge of protecting privacy in 21st Century America. In supporting the comprehensive approach, you are "moving the bar higher" for this Congress. You are also offering hope to the millions of Americans who want stronger legal protection for their personal data.

In addition to protecting the personal data of all Americans, a strong national privacy policy advances several societal interests. By ensuring that personal information is only used in a fair manner, citizens can more securely participate in economic, community and political activities. Clearly, consumer privacy concerns proved to be a major impediment to e-commerce. What many people failed to realize

was that a "privacy-first" policy was fundamental to the health of e-commerce, not a detriment to it.

Moreover, we must put in place a privacy-first policy if we are to enjoy the benefits—and the potentially tremendous cost savings—of the electronic age. Nearly all governmental and corporate organizations can dramatically reduce their costs and provide more efficient service if they can move from a paper environment to an electronic one. But consumers will not participate widely in electronic environments until they are convinced their privacy will be respected, and protected. In other words, we cannot afford not to adopt a comprehensive privacy policy.

When it comes to privacy legislation, specifics and details are paramount. I, and other members of the Privacy Coalition, look forward to working with you and the Subcommittee to ensure that the specific provisions of S. 1055 stay true to its purpose of comprehensive privacy protection. Many coalition members, including the Privacy Rights Clearinghouse, Electronic Privacy Information Center, Consumers Union and U.S. PIRG will be able to provide specific recommendations for making your bill even more effective at protecting Americans' cherished right to privacy.

WHY LEGISLATION IS URGENTLY NEEDED

A brief look at history helps explain why there is such a large gap between the comprehensive privacy protection we should have and the inadequate system currently in place.

Because of the Fourth Amendment of the U.S. Constitution, which guaranteed Americans that they would be secure in their personal papers, the United States emerged as a world leader in privacy. At the beginning, most personal data were kept at home in desks or lock boxes.

In the 20th Century, however, a vast system of third-party record keeping arose. Personal information was collected and maintained by banks, doctors and hospitals, credit reporting agencies, pharmacies, utilities, insurers, employers and government agencies.

In 1976, the U.S. Supreme Court, in *U.S.* v. *Miller*, ruled that Americans did not have a Constitutional right to privacy in personal data held by third parties. It reasoned that when you open a bank account, you surrender your data to the flow of commerce. Absent statutory protection, the bank is more or less free to give your financial data to whomever it pleases. The bottom line was even though the information was about you, those that collected it and kept it, owned it. The Supreme Court ultimately extended this reasoning to telephone records and to the garbage.

One year later, in 1977, a bipartisan commission created by President Ford and Congress when it enacted the Privacy Act, recommended a comprehensive legislative package, concluding that protections were needed in such areas as financial, medical, communications and government records and Social Security numbers. It also recommended what every other Western country now has: a national office to oversee and enforce privacy policy. Unfortunately, most of the recommendations were not carried out.

Since then, Congress generally has responded to "narrow" privacy-related problems or anecdotes with narrow solutions. The result has been a hit-or-miss patchwork of laws that have left huge gaps. As I was the first to point out in 1990, America was the only nation with a law to protect the privacy of video rental records, but without a law to protect medical records. Such gaps, and the lack of a reliable enforcement mechanism, are key reasons why the European Union is concerned about the adequacy of U.S. privacy law and may someday have to restrict the flow of personal data about European citizens to the U.S.

PROBLEMS MOUNTING, HIGHER & DEEPER

In the first debates of the late 1970s, opponents argued that privacy legislation was not necessary because there was "no evidence of harm." Now, evidence of harm abounds.

Identity theft is said to be the fastest growing crime, climbing from a handful of cases in the early 1990s to 500,000 cases per year now. ID thieves bribe clerks, steal from mailboxes, filch data from computers and from the garbage and raid personnel files.

The underworld of "carders," that is, hackers, who specialize in stealing and selling credit card numbers, is steadily growing. Some are connected to organized crime groups in Russia, Eastern Europe and Nigeria. Victimized Web sites include Western Union, Egghead, CD Universe and CreditCards.com. Sources say that only a fraction of carder successes are known to the public. (see Bob Sullivan's excellent reporting at MSNBC.com)

Identity thieves are using stolen credit card numbers to buy names, addresses and SSNs from legitimate information brokers, and then use the fraudulently-purchased identifiers to commit identity theft. (see Washington Post, May 31, 2001)

Financial institutions basically have ignored federal regulators' recommendation that they guard against would-be privacy invaders by asking customers for PINs or passwords before giving out their personal data. (see Washington Post, July 23, 2001)

A computer hacker or hackers compromised the customer records of more than 100 online banks by attacking the servers of the S1 Corp., which serviced the online banks. The S1 Corp. declined to confirm which banks were compromised, and it's not clear how many of the banks informed their customers. An expert said the S1 case was "only a drop in the bucket." (see Privacy Times, July 23 & Securityfocus.com, July 6, 2001)

A pornographic Web site operator in California made $38 million by purchasing 800,000 credit card numbers, ostensibly for account verification, and then using the numbers to charge cardholders $19.95 for visiting his Web site. In 1999, a convicted felon similarly bought credit card numbers from Charter Pacific Bank.

Financial institutions continue to participate in telemarketing schemes in which customers are solicited for 30-day free trials and memberships, and then the telemarketer either charges it to the customer's credit card or adds a monthly charge to his or her mortgage statement.

GROWING PUBLIC SUPPORT FOR PROTECTION

Opinion polls have shown consistent support for privacy legislation, and steady concern that privacy is not adequately protected.

A 2001 Forrester Research survey found that 70% of the respondents were either "extremely" or "very" interested in seeing Congress pass Internet privacy legislation.

- A June 2001 poll conducted by the Gallup organization has found that 66% of Internet users think that the government should pass laws protecting privacy. The poll also found that frequent Internet users and individuals under the age of 50 were among the strongest supporters of such laws.
- In August 2000, Pew Internet & American Life Project found two major points of consistency: Internet users want a guarantee of privacy when they go online and many consumers are unaware of how privacy invasions take place and are consequently unable to take advantage of available privacy-enhancing technologies. Another finding of the report is that 86% of Internet users surveyed support an opt-in standard for the collection of personal information. (*"Trust and privacy online: Why Americans want to rewrite the rules"*)
- A series of opinion polls conducted by Alan Westin, of Privacy & American Business, showed high consumer concern. For instance, a December 1998 survey found that 82% of consumers say they have lost all control over how personal information is used by companies (with 50% agreeing "strongly ") and 61% do not believe that their rights to privacy as a consumer are adequately protected by law or business practices.
- Several members of the Al-Qaeda terrorist network supported their operations through identity theft, credit fraud and skimming. In fact, Al-Qaeda had a top-level committee devoted to identity theft, chiefly for passport fraud.

S 1055

S 1055 is an excellent starting point because 1) it takes one of the most comprehensive approaches to date; 2) it is largely based upon the standard which must drive all privacy law: affirmative, informed consent and 3) it requires, at a minimum, notice and opt-out for personal data that are not currently protected by federal law.

The strength of the bill is its creation of a strong privacy standard for information that most Americans feel is private and should not be used for secondary purpose without their consent: financial, medical, drivers and SSNs. Also attractive is the private right of action for SSNs, which I favor being expanded to other parts of the bill. A private right of action (PROA) is vital because it is not practical for one entity to enforce privacy law in each and every case; individuals must be empowered to defend their own rights. A PROA accomplishes this, and has proven effective in the Fair Credit Reporting Act and the Telephone Consumer Protection Act.

The bill appropriately envisions enforcement roles for the Federal Trade Commission and the State Attorneys General.

SOCIAL SECURITY NUMBERS (SSNS)

The bill should establish that only those entities currently and specifically authorized by law to collect SSNs may continue to demand consumers' SSNs, and that those entities not specifically authorized may not demand an individual's SSN.

Secondly, the bill should have an "anti-coercion" provision so that there are penalties for attempting to condition the use of goods or services on the basis of the individual providing an SSN.

LIMIT EXCEPTIONS FOR LAW ENFORCEMENT

The bill includes too many exceptions for law enforcement access to personal data without notice to the individual. On this issue, it would be preferable to follow the model of the Right to Financial Privacy Act of 1978.

INDEPENDENT PRIVACY OFFICE

In keeping with the bill's comprehensive approach, however, I strongly recommend that it be amended to create an independent national privacy office that can oversee the bill, investigate complaints and serve as a resource for the public and for the Congress. Every other Western nation has such an office; Canada has both a Federal Privacy Commissioner and Privacy Commissioners in each Province. These offices are usually small; for many years they had little or no regulatory authority. But the public gets tremendous value from them, in part because of their ability to shine the public light on questionable practices. Not having such an office has somewhat excluded the United States from the international privacy community. Members of Congress would find such an office increasingly valuable as constituents' complaints about privacy continue to mount. Such an office was proposed in legislation (S 1735) introduced in the 103rd Congress by Sen. Paul Simon.

PREEMPTION OF STATE LAW

A major issue in privacy debates is preemption of State law. I believe strongly that a strong, comprehensive national privacy law is the best, indeed the only, anecdote to a hodge-podge of inconsistent State laws. Passing good privacy laws in the States is not easy. Adoption of a strong national law would free the States to devote more time to other pressing issues. But until Washington can prove it is up to the job, it's premature to talk about prohibiting States from protecting the privacy rights of their citizens.

More importantly, we must engage a process in which State officials, including the State Attorneys General, governors, legislators and citizens groups, can evaluate whether a Federal proposal is satisfactory. If it is, the States voluntarily might commit to the Federal proposal. But presently, it would be profoundly undemocratic for Washington to dictate privacy policy to the States.

ACCESS

A fundamental aspect of privacy is guaranteeing individuals access to their personal data. This is a right already granted with respect to credit reports under the Fair Credit Reporting Act. We need to extend this right to all personal records and to exploit electronic technology to the benefit of consumers. Ensuring that consumers are "plugged into" their personal records is an important solution in the electronic age, particularly considering the need to regularly monitor your own profiles for unauthorized activity in order to prevent fraud or identity theft.

Again, thank you for this opportunity. I would be happy to answer any questions.

Statement of Hon. Strom Thurmond, a U.S. Senator from the State of South Carolina

Madame Chairwoman:

I am pleased that you are holding this hearing on the protection of private.information and the enormous problems associated with identity theft. Privacy of personal information is important to all Americans, especially in an age when details of financial transactions can be sent all over the world in an instant. It is important that Congress enact legislation that will protect personal identifiers, but at the same time will allow for the legitimate conduct of the business community and government agencies. I hope to work with my colleagues to develop a comprehensive

and reasonable piece of legislation that will deter identity theft by eliminating.the unauthorized access of personal information.

Identity theft occurs when an individual obtains the personal information of a victim, such as a social security number or a date of birth, and uses that information to open accounts and establish lines of credit. In effect, a person with access to another's social security number can pretend to be a different person. Usually, the victim does not discover the fraud-before the identity thief has substantially damaged the victim's credit. The victim must then go through a long and arduous process to correct the situation.

Unfortunately, the crime of identity theft appears to be on the rise. According to the testimony of Consumers Union, there were 500,000 to 700,000 victims of identity theft last year. Moreover, the number of complaints received by the Federal Trade Commission in December of 2001 was almost double the complaints received in March of the same year. The increasing prevalence of this crime is unacceptable.

Congress has addressed this issue in the past. The Identity Theft Act of 1998 established identity theft as a distinct crime and provided for punishment of fines and jail time. This Act gave law enforcement an important tool in the prosecution of identity theft. While the 1998 Act was a momentous step, we must do more than prosecute the thieves. We must also make it more difficult for these lawbreakers to. access personal information. Without access to personal information, there would be no identity theft, and thousands of Americans would no longer be victimized.

One of the primary ways in which identities are stolen is by use of the social security number. Unfortunately, the social security number is ubiquitous and is used for many purposes other than its originally intended use. It is routinely used as an identification number by health care professionals, educational institutions, and many private businesses. People are often pressured into providing this very sensitive number, never knowing who may ultimately be given access to their personal information.

I am therefore strongly in support of several of the Chairwoman's proposals regarding social security numbers. For example, one proposal would prohibit companies from selling social security numbers to the public. Congress should close all avenues to the sale of social security numbers and conduct appropriate oversight to ensure that violators are prosecuted. Another good proposal would require Social Security numbers to be redacted from public documents. Where feasible, Congress should cut off the public access of social security numbers. Yet another suggested reform would prohibit private companies from denying.service to individuals who refuse to provide social security numbers, with specific exceptions for transactions such as those that-involve credit checks. Most businesses have no legitimate need for social security numbers. Rather, the numbers are used for purposes such as identification and filing. Surely, there are other identification methods that could be developed easily, ensuring that social security numbers are not available to persons who would misuse them.

Many victims do not know how a social security number was stolen. I believe that Congress should respond by limiting the public use of this number. While no law will eliminate all instances of identity theft, Congress can and should make it more difficult for thieves to obtain an individual's personal information.

Madame Chairwoman, I am very interested in the bill introduced. I will carefully consider your the witnesses today in hopes of action. I will also on identity theft that will future. We should do all we can to limit the use of personal identifiers so that the growing problem of identity theft will be extinguished. I thank the Chairwoman for taking an interest in this important matter, that you have proposals and the testimony of determining the best course closely examine the GAO report be released in the near and I look forward to working with you.